3ème année

Sécurité des Systèmes Informatiques

SUPAERO

Rodolphe Ortalo
RSSI - CARSAT Midi-Pyrénées
rodolphe.ortalo@free.fr
(rodolphe.ortalo@carsat-mp.fr)
http://rodolphe.ortalo.free.fr/ssi.html

Présentation du cours (1/2)

- Généralités
  - Propriétés de sécurité
  - Attaques
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - Suivi des alertes de sécurité
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - Cryptographie
  - Politiques de sécurité formelles
  - Critères d'évaluation normalisés
- Sécurité et développement

Présentation du cours (2/2)

- Protection utilisées dans la pratique
  - Protection réseau et *firewall*
  - Systèmes d'authentification
  - Chiffrement de flux et VPN
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
  - Détection d'intrusion
  - Audit, tests d'intrusion
  - Administration, exploitation et suivi de la sécurité
  - Observation et surveillance
- Protection des applications usuelles

Plan (1/2)

- **Généralités**
  - Propriétés de sécurité
  - Attaques
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - Suivi des alertes de sécurité
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - Cryptographie
  - Politiques de sécurité formelles
  - Critères d'évaluation normalisés
  - Principes de conception et d'utilisation

Sécurité et Malveillances

- Protection d'un système vis à vis d'un adversaire

security vs. *safety* (engl.)

Un large périmètre d'action

- Actions non-techniques
  - Habilitation des personnes
  - Délégation écrite
  - Contrats
  - Sensibilisation / Formation
  - Enseignement
- Protection
  - Réseau
  - Système
  - Applications
- Surveillance
  - Détection d'intrusion
  - Observation
- Connaissance des agressions
  - Attaques
  - Vulnérabilités / Audit
  - Tests d'intrusion
- Gestion des risques et évaluation

Technologies concrètes

- Firewall
- Détection d'intrusion
- Systèmes d'authentification
- VPN
- Protection des applications
- Administration
- Utilitaires « sécurité » (intégrité, chiffrement, etc.)
- Observation et surveillance réseau

Plan (1/2)

- Généralités
  - **Propriétés de sécurité**
  - Attaques
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - Suivi des alertes de sécurité
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - Cryptographie
  - Politiques de sécurité formelles
  - Critères d'évaluation normalisés

Propriétés de base - **Confidentialité**

- Propriété d'une information de ne pas être révélée à des utilisateurs non autorisés à la connaître
  - empêcher les utilisateurs de lire une information confidentielle, sauf s'ils y sont autorisés
  - empêcher les utilisateurs autorisés à lire une information confidentielle de la divulguer à des utilisateurs non-autorisés

Propriétés de base - **Intégrité**

- Propriété d'une information d'être exacte
  - empêcher une modification (création ou destruction) indue de l'information (incorrecte ou par des utilisateurs non autorisés)
  - faire en sorte qu'aucun utilisateur ne puisse empêcher une modification légitime

Propriétés de base - **Disponibilité**

- Propriété d'une information d'être accessible quand on en a besoin
  - fournir l'accès à l'information pour que les utilisateurs autorisés puissent la lire ou la modifier
  - faire en sorte qu'aucun utilisateur ne puisse empêcher les utilisateurs autorisés d'accéder à l'information

L'information

- Données
  - saisies, générées, stockées, transmises, affichées, ...
- « Méta-données » : associées aux données et utilisées par les services de manipulation
  - identités, noms, adresses (utilisateur, machine, processus, périphériques, etc.)
  - temps (date de l'opération)
  - droits d'accès
  - etc.

Autres propriétés

- Anonymat = confidentialité de l'identité d'un utilisateur
- Protection de la vie privée = confidentialité de (données personnelles + identité de l'utilisateur)
- Authenticité d'un message = intégrité du (contenu + identité de l'émetteur + date + …)
- Authenticité d'un document = intégrité du (contenu + identité du créateur + date + …)
- Authenticité d'un utilisateur = intégrité de l'identité
- « Auditabilité » = disponibilité de (qui, quoi, quand, où, …) d'une action
- Non-répudiation d'origine = disponibilité de (identité de l'émetteur + …) + intégrité du contenu
- Non-répudiation de réception = disponibilité de (identité du récepteur + …) + intégrité du contenu
- Protection de la propriété intellectuelle = confidentialité du contenu (+ intégrité du contenant)

Besoins de sécurité selon les secteurs

- Défense, gouvernement :
  confidentialité $\gg$ intégrité, disponibilité
- Finance :
  intégrité $\gg$ disponibilité > confidentialité
- Autres : industrie, administrations, médecine
  ça dépend !

 Il faut définir les besoins spécifiques de l'application : Politique de sécurité

Axes d'action théoriques

- Prévention
  - La prévention des fautes vise à empêcher l'occurrence ou l'introduction de fautes.
- Tolérance
  - La tolérance aux fautes correspond à un ensemble de moyens destinés à assurer qu'un système remplit sa fonction en dépit des fautes.
- Élimination
  - L'élimination des fautes vise à réduire le nombre ou la sévérité des fautes.
- Prévision
  - La prévision des fautes vise l'estimation de la présence, la création et les conséquences des fautes.

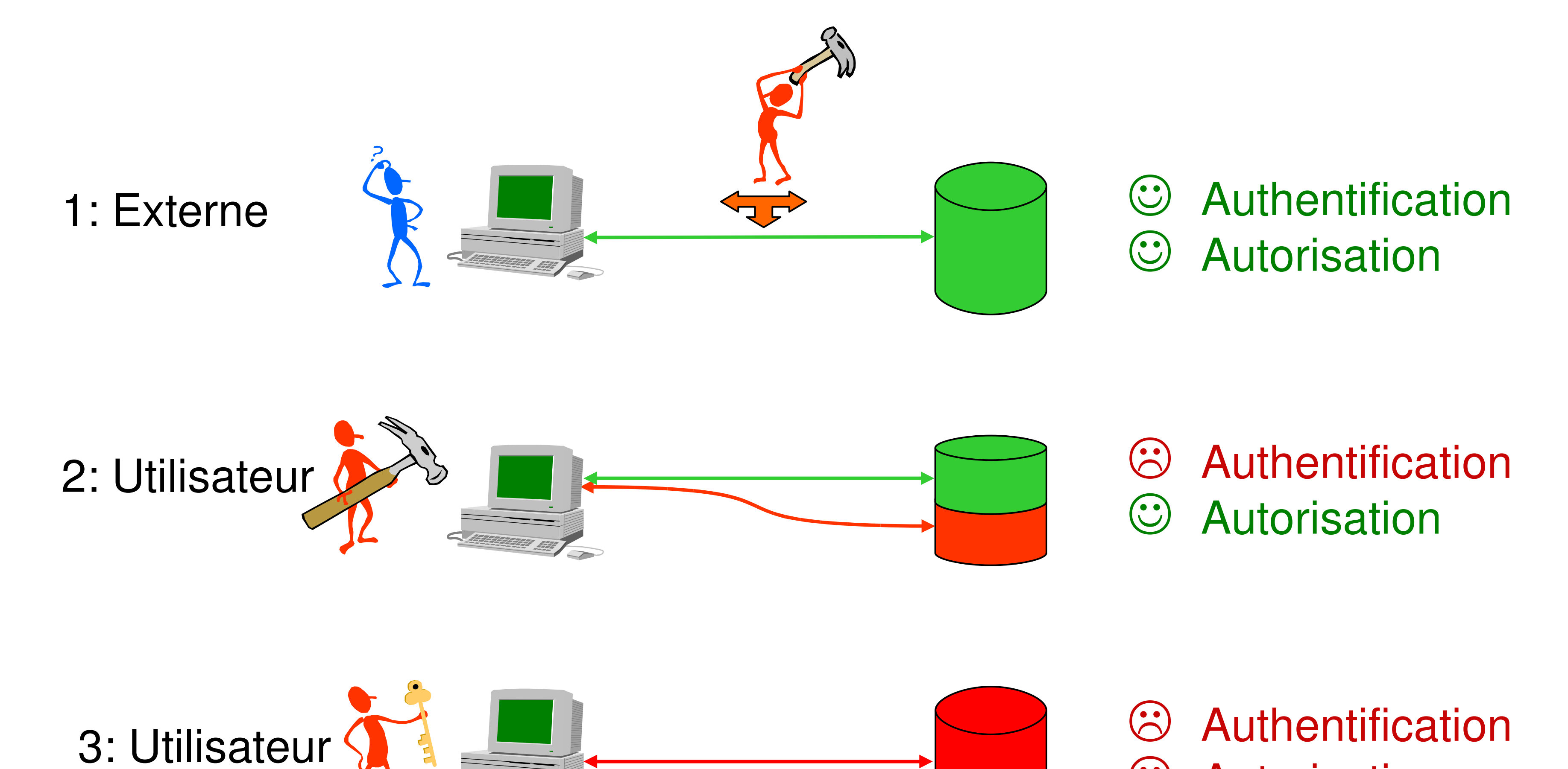
Plan (1/2)

- Généralités
  - Propriétés de sécurité
  - **Attaques**
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - Suivi des alertes de sécurité
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - Cryptographie
  - Politiques de sécurité formelles
  - Critères d'évaluation normalisés

Les attaquants et leurs motivations

- Jeu : explorer les limites, éprouver et étendre ses connaissances, découvrir de nouvelles failles, améliorer la sécurité : "hackers" (pirates = "crackers" en fait)
- Émulation, sectarisme : groupe de hackers : "exploits"
- Vandalisme : montrer sa force, punir : "web defacing", virus, vers…
- Politique, idéologie : ex. CCC
- Vengeance
- Profit : espionnage, extorsion de fonds : concurrence déloyale, crime organisé
- Guerre informatique, terrorisme ?
- Sensibilisation, lobbying
- Protection abusive : ex. SONY

Qui sont les « intrus »?



80% des fraudes sont "autorisées"

Caractériser des attaquants
[ITSEM 1993, §3.3.29-32, §6.C.28-34]

- compétence
  - profane
  - personne compétente
  - expert
- ressources
  - temps
    - quelques minutes
    - quelques jours
    - quelques mois
  - équipement
    - sans équipement
    - équipement disponible
    - équipement spécial
- opportunités
  - collusion
    - seul
    - avec un utilisateur
    - avec un administrateur
  - chance
  - détection

Niveau de résistance
- élémentaire
- moyenne
- élevée

Des classes d'attaques

- Ecoute passive
- Interception
- Canaux cachés
- Cryptanalyse
- Répudiation
- Inférence
- Déguisement
- Portes dérobées
- Bombe logique
- Cheval de Troie
- Virus
- Ver
- Déni de service
- et attaques complexes...

Bénéfices envisageables

- Gains financiers :
  - Utilisation de numéros de cartes de crédit
  - Chantage, extorsion de fonds, espionnage industriel, …
  - Connexion à des lignes téléphoniques payantes
  - Accès à des comptes (banques, *paypal*, FAI, opérateurs téléphoniques, hotspots, retraites…)
  - Vente d'adresses e-mails : ex. 28 000 $ pour 92 M@ (AOL)
  - Services payants (ex. porno, films piratés…) + *spammers*, …
  - *click fraud* (relais de publicité) : ex : 60 K$ avec 0,4 Mpc
  - Location de botnets, …2004: (IRC) #botz4sale

➔ Correction des failles pour protéger ses revenus

Exemple de phishing



Perfectionnement de Banque AGF en ligne

Cher Client,

Nous poursuivons le perfectionnement de notre site web. Comme vous le savez certainement, Banque AGF vous offre un mécanisme idéal pour une gestion optimisée de votre argent au quotidien.

Chaque jour, nous travaillons pour améliorer notre système et nous voulons vous communiquer les résultats de nos efforts :

- Maintenant, lorsque le solde de votre compte dépasse 750 €, l'exc édent est automatiquement transféré sur votre Compte sur Livret pour vous rapporter des intérêts en restant disponible à tout moment

- Si vous n'avez pas de contrat d'assurance avec Banque AGF, il est temps d'y penser, car vous bénéficierez de conditions privilégiées en passant par notre banque à distance. Découvrez la gamme Privalis maintenant!

- Banque AGF vous présente l'occasion de donner vie à vos projets – les crédits auto et immobiliers sont désormais disponibles 24h/24 et 7j/7. Pour les abonnés de Banque AGF à distance les prêts Reflexis commencent à 2.90% TEG fixe.

- Etez-vous néophite en bourse? Banque AGF en ligne vous présente un guide complet qui vous permettra de comprendre les mécanismes boursiers ainsi que les termes spécifiques. Vous saurez la différence entre les actions nominatives et les bons de souscription et pourrez même acheter des actions en ligne de votre domicile.

De plus, nous avons une offre spéciale pour ceux qui travaillent en situation de mobilité externe, c'est-à-dire avec des assistants numériques personnels (PDA) ou des téléphones portables multifonctions. Dès aujourd'hui vous pouvez consultez vos comptes en utilisant ces appareils.

Pour pouvoir profiter de toutes les nouvelles options, veillez confirmer vos données en passant par le lien en bas de cette page.

Veuillez agréer l'assurance de notre considération distinguée,

Banque AGF

© 2005 Banque AGF.

Exemple de phishing (2)

De : PayPal <account.access@paypal.com>
Objet : **Update Your PayPal Account**
Date : 15 novembre 2005 04:38:35 HNEC
Répondre à : no.reply@paypal.com



Dear valued **PayPal®** member:

It has come to our attention that your **PayPal®** account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension.

Once you have updated your account records, your **PayPal®** session will not be interrupted and will continue as normal.

To update your **PayPal®** records click on the following link:
http://www.paypal.com/cgi-bin/webscr?cmd=_login-run

http://61.56.224.108/.cgi-bin/index.php

Thank You.
PayPal® UPDATE TEAM



Accounts Management As outlined in our User Agreement, **PayPal®** will periodically send you information about site changes and enhancements.

PayPal - Sign Up - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://34.436.54.876

PayPal

Sign Up | Log In | Help

Welcome | Send Money | Request Money | Shop | Sell

Personal Account Verification - Just 1-Page! Personal | Business | International Sign Up

Your Profile Information - This will be processed by PayPal. Your information will be kept secure and private. secure and private.

First Name:
Last Name:
Address 1:
Address 2: (optional)
City:
State:
Zip: (5 or 9 digits)
Country: U.S.A. Outside the U.S.?
Home Telephone: Kept Private Kept Private
Work Telephone: (optional)

Your Email Address and Password - Enter the e-mail address and password which you use to login to PayPal.

Email Address:
Password:

Credit Verification - Enter the credit card information which you use with PayPal. Please make sure that you have entered this information correctly, as your account will not be re-activated if it is wrong.

Cardholder's Name:
Credit Card Number - - -
Expiration Date: (01) January 2002
Zip/Postal Code: (5 or 9 digits)
Security Code: (On the back of your card, locate the final 3 digit number) Help finding Card Verification Number Help finding Card Verification Number | Using Amex? Using Amex?

Additional Security Info - In order to fully validate your account, we ask that you fill in some extra security information. We assure you this information is kept confidential.

Social Security Number:
Date of Birth: (mm/dd/yyyy)
Mother's Maiden Name:
Issuing Bank:
ABA Number (bank branch number)
Account Type ◉ Checking ○ Savings
Routing Number
This is the number located between the symbols.
Account Pin: (4 digit number * must enter)
Account Number:
Typically comes before the symbol. Its exact location and number of digits varies from bank to bank.

Use the image below to enter your account number and routing number.

U.S. Check Sample
Routing Number | Check # | Account Number
211554485 0012 1456874801

By clicking "Continue", I agree to be bound by PayPal's User Agreement. User Agreement. Sign Up

About Us | Accounts | Fees | Privacy | Security Center | User Agreement |

an eBay company

Information about FDIC pass-through insurance

Exemple de *scam*

DEAR SIR,

URGENT AND CONFIDENTIAL BUSINESS PROPOSAL

I AM MARIAM ABACHA, WIDOW OF THE LATE NIGERIAN HEAD OF STATE, GEN. SANI ABACHA. AFTER HE DEATH OF MY HUSBAND WHO DIED MYSTERIOUSLY AS A RESULT OF CARDIAC ARREST, I WAS INFORMED BY OUR LAWYER, BELLO GAMBARI THAT, MY HUSBAND WHO AT THAT TIME WAS THE PRESIDENT OF NIGERIA, CALLED HIM AND CONDUCTED HIM ROUND HIS APARTMENT AND SHOWED HIM FOUR METAL BOXES CONTAINING MONEY ALL IN FOREIGN EXCHANGE AND HE EQUALLY MADE HIM BELIEVE THAT THOSE BOXES ARE FOR ONWARD TRANSFER TO HIS OVERSEAS COUNTERPART FOR PERSONAL INVESTMENT.

ALONG THE LINE, MY HUSBAND DIED AND SINCE THEN THE NIGERIAN GOVERNMENT HAS BEEN AFTER US, MOLESTING, POLICING AND FREEZING OUR BANK ACCOUNTS AND EVEN MY ELDEST SON RIGHT NOW IS IN DETENTION. MY FAMILY ACCOUNT IN SWITZERLAND WORTH US$22,000,000.00 AND 120,000,000.00 DUTCH MARK HAS BEEN CONFISCATED BY THE GOVERNMENT. THE GOVERNMENT IS INTERROGATING HIM (MY SON MOHAMMED) ABOUT OUR ASSET AND SOME VITAL DOCUMENTS. IT WAS IN THE COURSE OF THESE, AFTER THE BURIAL RITE AND CUSTOMS, THAT OUR LAWYER SAW YOUR NAME AND ADDRESS FROM THE PUBLICATION OF THE NIGERIAN BUSINESS PROMOTION AGENCY. THIS IS WHY I AM USING THIS OPPORTUNITY TO SOLICIT FOR YOUR CO-OPERATION AND ASSISTANCE TO HELP ME AS A VERY SINCERE RESPONSIBLE PERSON. I HAVE ALL THE TRUST IN YOU AND I KNOW THAT YOU WILL NOT SIT ON THIS MONEY.

I HAVE SUCCEEDED IN CARRYING THE FOUR METAL BOXES OUT OF THE COUNTRY, WITH THE AID OF SOME TOP GOVERNMENT OFFICIAL, WHO STILL SHOW SYMPATHY TO MY FAMILY, TO A NEIGHBOURING COUNTRY (ACCRA-GHANA) TO BE PRECISE. I PRAY YOU WOULD HELP US IN GETTING THIS MONEY TRANSFERRED OVER TO YOUR COUNTRY. EACH OF THESE METAL BOXES CONTAINS US$5,000,000.00 (FIVE MILLION UNITED STATES DOLLARS ONLY) AND TOGETHER THESE FOUR BOXES CONTAIN US20,000,000.00(TWENTY MILLION UNITED STATESDOLLARS ONLY). THIS IS ACTUALLY WHAT WE HAVE MOVED TO GHANA.

THEREFORE, I NEED AN URGENT HELP FROM YOU AS A MAN OF GOD TO HELP GET THIS MONEY IN ACCRA GHANA TO YOUR COUNTRY. THIS MONEY, AFTER GETTING TO YOUR COUNTRY, WOULD BE SHARED ACCORDING TO THE PERCENTAGE AGREED BY BOTH OF US.PLEASE NOTE THAT THIS MATTER IS STRICTLY CONFIDENTIAL AS THE GOVERNMENT WHICH MY LATE HUSBAND WAS PART OF IS STILL UNDER SURVAILLANCE TO PROBE US.

YOU CAN CONTACT ME THROUGH MY FAMILY LAWYER AS INDICATED ABOVE AND ALSO TO LIAISE WITH HIM TOWARDS THE EFFECTIVE COMPLETION OF THIS TRANSACTION ON TEL/FAX N0:xxx-x-xxxxxxx AS HE HAS THE MANDATE OF THE FAMILY TO HANDLE THIS TRANSACTION.

THANKS AND BEST REGARD

MRS. MARIAM ABACHA

☹ Parfois: recel et blanchiment d'argent !

http://www.joewein.de/sw/spam.htm

Exemple : *Cross Site Scripting*

http://www.cert.org/advisories/CA-2000-02.html

- Un pirate crée un script caché dans un message (ex: HTML tags "`SCRIPT`" et "`/SCRIPT`").
- Il l'enregistre sur un serveur innocent (ex: blog, forum, …).
- La victime lit le message avec un browser configuré pour permettre l'exécution de scripts...
- La victime peut aussi s'auto-scripter (ex: par phishing) :

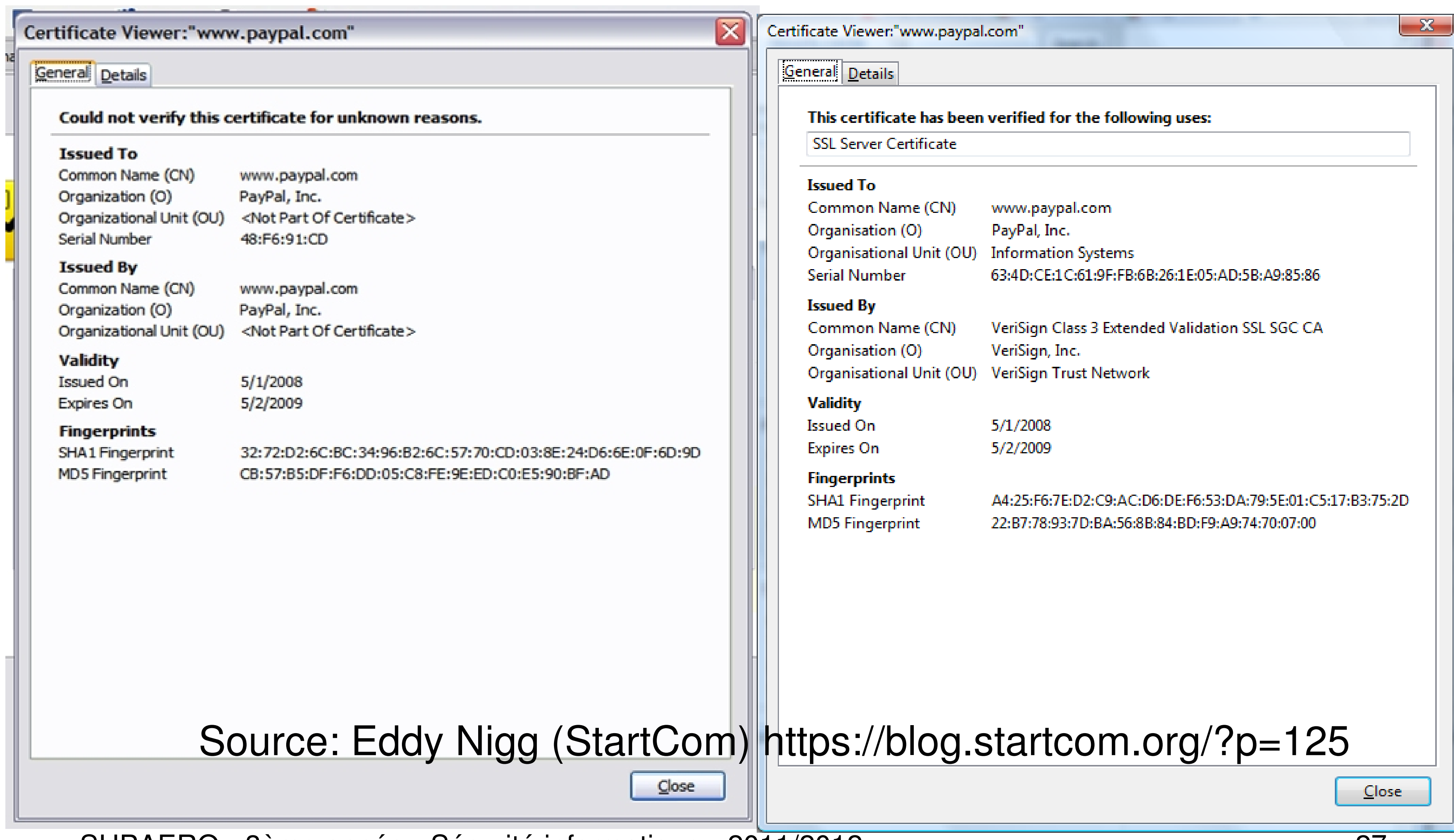
```
<A HREF="http://example.com/comment.cgi?
mycomment=<SCRIPT>malicious code</SCRIPT>"> Click here</A>
```

Falsification d'empreintes digitales

- Objectif : tromper un lecteur d'empreinte de PC
- Matériel
  - Verre propre
  - (Vapeur de) Colle cyanocrylate
  - Appareil photo numérique
  - PC, imprimante laser, transparent
  - Colle à bois

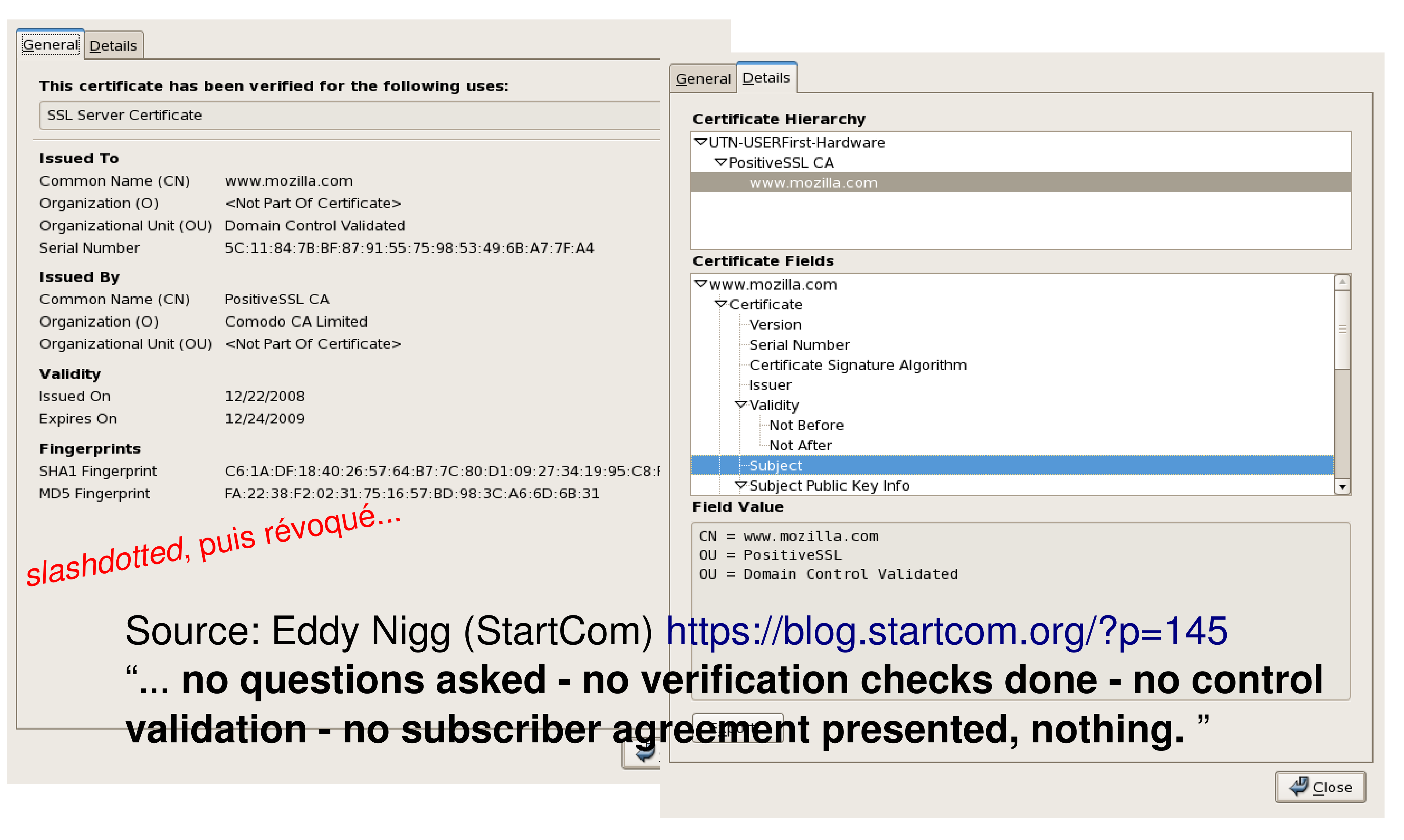
    http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en
- Et c'est là une méthode « sophistiquée » (par opposition à la pâte à modeler, la buée)

Présentation et certificats



Source: Eddy Nigg (StartCom) https://blog.startcom.org/?p=125

Délivrance des certificats



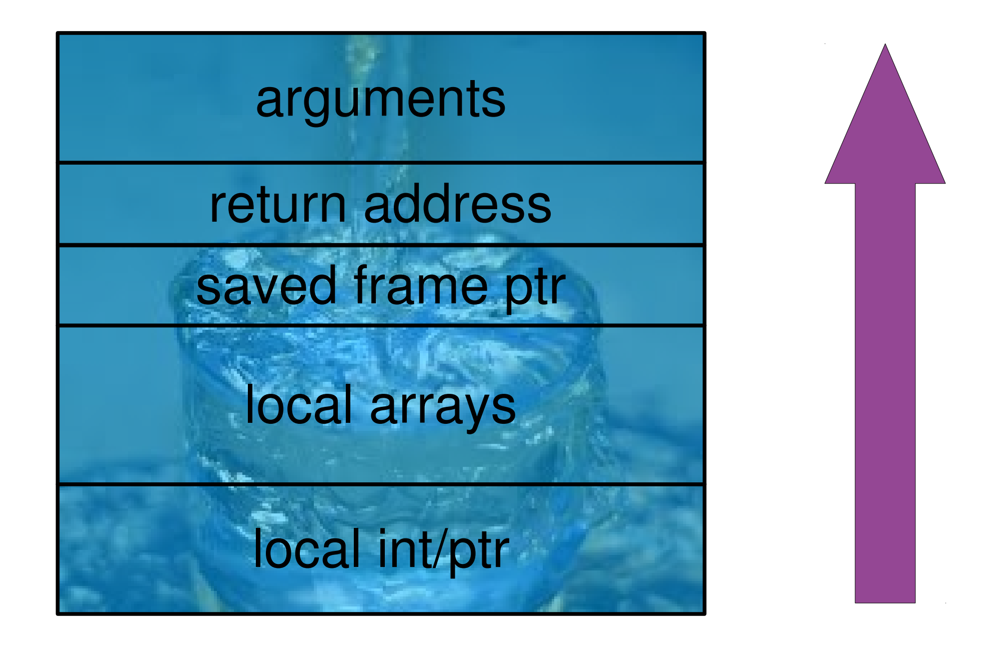
Source: Eddy Nigg (StartCom) https://blog.startcom.org/?p=145

"... no questions asked - no verification checks done - no control validation - no subscriber agreement presented, nothing. "

Buffer Overflow – Un exemple

- Fonctionnement d'un appel de fonction (C)
  - Sauvegarde des registres généraux sur la pile
  - Calcul de l'adresse de retour et sauvegarde sur la pile
  - Empilement des paramètres d'appel de la fonction
  - Les variables locales et les tableaux sont également stockés sur la pile
- L'ordre exact dépend du contexte, mais l'idée générale est toujours la même

Disposition de la pile



Contrived example

```
void function(char* str) {
   char buffer[16] ;
   strcpy(buffer, str) ;
 }
int main(void) {
   /* lenght of str > 16 bytes */
   char* s = "Je ne fais pas moins de 16
   caractères.";
   function(s) ;
}
```

Vulnérabilité de ce type de code?

- Le résultat n'est pas toujours prévisible
- On écrit dans des zones mémoires non prévues pour cela
- Avons-nous écrasé l'adresse de retour ?
- Avec des valeurs d'entrées choisies très soigneusement, on peut fixer le point de retour de la suite du programme
- Cela peut se situer dans du code contrôlé par l'utilisateur, si celui-ci à réussi à la faire rentrer en mémoire.
  - Sinon, on se débrouille autrement

Format strings

```
int function(char* str) {
   fprintf(stdout, str) ;
}
```

- Que se passe t'il quand :

```
   str = "%s%s%s%s%s";
```

- Le plus probable : une erreur fatale
- Sinon : impression du contenu de la mémoire

- NB : forme correcte

```
   fprintf(stdout, "%s", str);
```

Prévention

- Attention en écrivant dans des tampons mémoire
  - Le contrôle de la longueur des entrées est obligatoire
- Ne jamais utiliser de trucs en C
- strcpy() et strcat() sont interdits
  - Utiliser strlcpy() et strlcat()
  - Si vous en disposez...

Hack1ng R0x

- Buffer overflows (exemple SSL, exemple)
- Format strings (exemple, exemple)
- Etc.

Lisez `Phrack`

- Une autre référence plus académique

How to 0wn the Internet in your Spare Time,
Staniford, Paxson, Weaver, 11th Usenix Security Symposium, 2002.

Actualités 2010

- Stuxnet
- Phishing visant la CAF
- Les états d'âmes de Linux
- Google part de Chine
- GSM et la sécurité

Some news 2010/2011
with 2012 update

- New or significant failures
  - Compromised, abused (Comodo, DigiNotar) or doubtful *Internet* certification authorities
    - *Business as usual or bankruptcy*
  - Intrusion at Bercy (G20 organization)
    - *nothing*
  - *Sony PlayStation Network*
    - Personal data of 77 millions users stolen
    - *« Welcome back » package, class action running*
  - STARS / Stuxnet
    - Very specific worm targeting critical industrial control systems
    - *NYT reports combined U.S./Israeli intelligence operation running under two different presidents (0*

Some news 2010/2011

- State communication
  - *La sécurité dans le cyberspace, un enjeu stratégique,* Lettre du Secrétaire Général de la Défense et de la Sécurité Nationale (SGDSN), fin 2010
  - Communication du Premier ministre relative à la protection des systèmes d’information au Conseil des ministres du 25 mai 2011
    - *ANSSI hires, gets a new building and plays Antigone...*
    - *ANSSI does cryptanalysis research (!)*
  - In summer 2011, the *Department of Transport* launched a call for proposals with respect to cars (cyber) security
    - *Summer 2012 : WiFi linked vehicle test*





Hackers interests



- Latest hackers security conferences (ie. DEFCON & BlackHat 2011)
  - Home automation security (especially X10 over CPL systems)
  - Car alarms
  - Insulin pumps
  - Autonomous WiFi+GSM sniffing drone

DEFCON 2012

- *NFCs, anti-forensics, gen. Keith Alexander*





Recent programmer comment

World-writable memory on Samsung Android phones

Posted Dec 17, 2012 20:13 UTC (Mon) by **mikov** (subscriber, #33179) [Link]

My experience from most places: nobody cares, nobody reviews. If a problem is discovered later, we will fix it later - why worry now and delay the release? What "/dev/mem"?? Enough with this mumbo-jumbo we have a release to make and management bonuses to earn.

In fact people who do care and worry about esoteric things like "security", or "good design" or "code quality" are universally viewed as trouble-makers or ivory tower idiots both by management and most of the engineers. It is an uphill battle even to do what used to be the baseline 10-15 years ago.

Commercial software engineering now is no different from accounting. The glory days are gone. It is all downhill from now on.

http://lwn.net/Articles/529496/

BTW, Cyanogen fix: http://review.cyanogenmod.org/#/c/28568/

Une dernière (moins récente)...

« The final step (…) simply adds a second Trojan horse to the one that already exists. The second pattern is aimed at the C compiler. The replacement code is a (…) self-reproducing program that inserts both Trojan horses in the compiler. (…) First we compile the modified source with the normal C compiler to produce a bugged binary. We install this binary as the official C. We can now remove the bugs from the source of the compiler and the new binary will reinsert the bugs whenever it is compiled. Of course, the login command will remain bugged with no trace in source anywhere. »

Morale

« *You can't trust code that you did not totally create yourself.*

(Especially code from companies that employ people like [him].) »

Ken Thomson, Reflections on Trusting Trust, *Turing award lecture*, in *Communications of the ACM*, vol.27, no.8, pp.761-763, August 1984.

Plan (1/2)

- Généralités
  - Propriétés de sécurité
  - Attaques
- Mise en œuvre dans les organisations
  - **Fonctionnement de la sécurité dans une entreprise**
  - Suivi des alertes de sécurité
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - Cryptographie
  - Politiques de sécurité formelles
  - Critères d'évaluation normalisés

Environnement de la SSI

- Internes ou associés
  - Service études
  - Service exploitation
  - Sous-traitants
  - Organismes nationaux
  - Tutelles
  - CE/DP
  - Service juridique
- Externes et indépendants
  - Justice
  - ANSSI (www.ssi.gouv.fr)
  - CNIL (www.cnil.fr)
  - CERT/CC (www.cert.org)
    US-CERT (www.us-cert.gov)
    CERTA (www.certa.ssi.gouv.fr)
  - CESTI
  - OCLCTIC
    (http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic)

Organisation dans une entreprise

- Un « responsable » (RSSI)
- Comité de sécurité informatique
- Groupes de travail
  - Mise en place de l'organisation SSI
  - Sensibilisation des utilisateurs
  - Audit et gestion des risques
  - Autorisation et actions de sécurité opérationnelle
  - Surveillance et contrôle
  - Veille technologique
  - *projet*
- Gestion de crise

Fonctions du RSSI

Cigref 2001

- Définition de la politique de sécurité
- Analyse de risques
- Sensibilisation et formation aux enjeux de la sécurité
- Étude des moyens et préconisations
- Audit et contrôle
- Veille technologique et prospective

Rôles de conseil, d’assistance, d’information, de formation et d’alerte.

Si possible indépendant de la direction informatique.

Différents documents

- Analyse des risques
- Politique de sécurité (PSSI)
- Spécifications de sécurité
- Guides de configuration ou de recette sécurité
- Synthèse/Suivi : alertes, filtrage, violations
- Tableau de bord ou audit/contrôle interne

Analyse des risques

1. Identifier les biens et leur valeur
2. Attribuer des priorités aux biens
3. Déterminer la vulnérabilité aux menaces et les dommages potentiels
4. Attribuer des priorités à l'impact des menaces
5. Sélectionner des mesures de protections rentables

(Le point de vue d'un informaticien incompétent en matière de droit sur la) Législation

- La protection des informations nominatives est forte et obligatoire en France (CNIL)
- L'utilisation du chiffrement est sujette à contrôle strict en France (DCSSI)
- Toutes les législations et conventions s'appliquent (au système d'information)
  - Lois, décrets, ordonnances, circulaires, …
  - Secret médical, secret bancaire, secret professionnel, …
  - Droit du travail, convention collectives, règlements intérieurs
  - Droit commercial, contrats, …
  - …
- La signature numérique est en attente de jurisprudence
- La preuve numérique également

  (Si, aprés MD5, SHA-1 tombe aussi, l'attente pourrait durer...)

Les actions concrètes du RSSI

- www.cert.org, www.us-cert.gov, www.certa.ssi.gouv.fr
- Paramétrage du *firewall*
- Animation du comité de sécurité et des groupes de travail
- Documentation (PSSI, guides, etc.)
- Interaction avec les organismes extérieurs

- Suivi des tests d'intrusion, gestion des autorisations

Traitement du risque ou simple gestion ?

L'Agence Nationale de la Sécurité des Systèmes d'Information en 2011



Des évolutions intéressantes:

http://www.ssi.gouv.fr/fr/anssi/publications/discours-de-patrick-pailloux-lors-de-la-conference-de-cloture-des-assises-de-la.html (lien local)

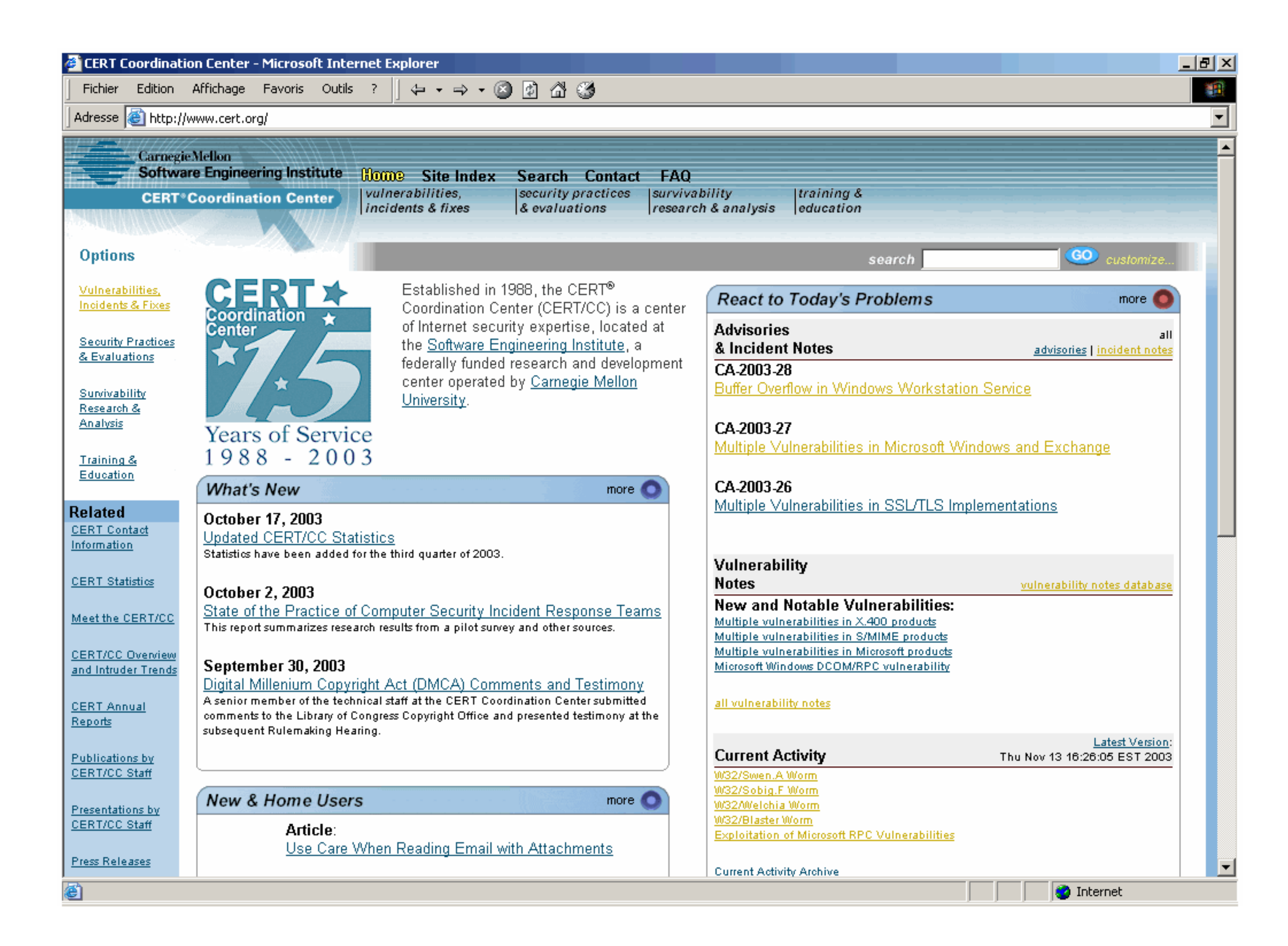
Plan (1/2)

- Généralités
  - Propriétés de sécurité
  - Attaques
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - **Suivi des alertes de sécurité**
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - Cryptographie
  - Politiques de sécurité formelles
  - Critères d'évaluation normalisés

Le CERT

Computer Emergency Response Team

www.cert.org



Principales informations diffusées

React to Today's Problems

more

Advisories & Incident Notes

all
advisories | incident notes

CA-2003-28
Buffer Overflow in Windows Workstation Service

CA-2003-27
Multiple Vulnerabilities in Microsoft Windows and Exchange

CA-2003-26
Multiple Vulnerabilities in SSL/TLS Implementations

Vulnerability Notes

vulnerability notes database

New and Notable Vulnerabilities:

Multiple vulnerabilities in X.400 products
Multiple vulnerabilities in S/MIME products
Multiple vulnerabilities in Microsoft products
Microsoft Windows DCOM/RPC vulnerability

all vulnerability notes

Current Activity

Latest Version:
Thu Nov 13 16:26:05 EST 2003

W32/Swen.A Worm
W32/Sobig.F Worm
W32/Welchia Worm
W32/Blaster Worm
Exploitation of Microsoft RPC Vulnerabilities

Current Activity Archive

Les avis et notes du CERT

- Avis (exemples)
  - CERT Advisory CA-2003-28 (Microsoft)
  - CERT Advisory CA-2003-26 (SSL/TLS)
- Base de vulnérabilités
  - CERT VU#567620 (de CA-2003-28 et Microsoft MS03-049) http://www.kb.cert.org/vuls/id/567620
  - CA-2003-26 est associé à 6 vulnérabilités
  - CERT VU#936868 (Oracle et réplique) http://www.kb.cert.org/vuls/id/936868
  - Avis constructeurs et autres: http://www.debian.org/security/2004/dsa-419

Tous les avis

Fiche CERT : Principaux éléments

- *Title / Overview*
- *Systems affected*
- *Description*
- *Impact*
- *Solution*
- *References*
- *Credit / Vendor Info. / Other Info.*

La série Blaster (été 2003)

- CERT VU#568148
- CERT Advisory CA-2003-16
- Microsoft MS03-026
- CERT Advisory CA-2003-19
- CERT Advisory CA-2003-20
- CERT Current Activity (Blaster)

L'actualité plus récente

- CERTA, hier :
  - Page principale

  - La dernière blague de Windows
  - Back to SSL conception
  - etc.

Plan (1/2)

- Généralités
  - Propriétés de sécurité
  - Attaques
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - Suivi des alertes de sécurité
  - **Définition d'un schéma directeur sécurité**
- Mécanismes de protection généraux
  - Cryptographie
  - Politiques de sécurité formelles
  - Critères d'évaluation normalisés
  - Principes de conception et d'utilisation

Schéma directeur SSI

- Ensemble documentaire constitué par
  - PSSI (Politique de sécurité du syst. d'info.)
  - Spécifications ou règlements de sécurité par domaine
    - réseau, système, SGBD, développement, marchés, etc...
  - Guides pratiques et/ou points de validation
    - AIX 5.x, W2K Server SP4, IOS 12.x, Apache 1.2, etc.
  - Dossiers de sécurité des applications
    - paye, achats, compta., métier 1, métier 2, etc.
  - Gestion des risques (audit, suivi)
  - Tableau de bord
  - Plan d'action

PSSI

- Structure
  - Organisation et responsabilités
  - Intégration et interactions de la SSI
    - SSI et projets
    - SSI et exploitation
  - Objectifs de sécurité de l'organisme
  - Règles générales de sécurité
  - Gestion des risques

Modèle de PSSI diffusé par la DCSSI

- Domaines d'application
  - Communications
  - Violations
  - Vie privée
  - Achats de matériels
  - Messagerie
  - Maintenance
  - Audit
  - Communications
  - Identification
  - Authentification
  - Surveillance
  - Contrôle d'accès
  - Disponibilité
  - Réseau
  - …

Caractéristiques d’une bonne PSSI

- Réaliste
- Applicable
- Vision à long terme
- Clarté et concision
- Basée sur des rôles ou des profils
- Définition claire des domaines de responsabilité et d’autorité
- À jour (revue périodiquement)
- Communiquée à tout le personnel

« Spécifications »

- Spécifications de sécurité
  - Clauses contractuelles
  - Charte déontologique et utilisateurs (finaux, administrateurs, etc.)
  - Composants réseau
  - Systèmes
  - Collecte des traces et « cybersurveillance »
  - Systèmes d'authentification
  - Application (*X*, *Y*, *Y*, etc.)
  - Données (*A*, *B*, *C*, *D*, etc.)

Documents opérationnels

- Guides de configuration / Points de contrôles
- Déclinés précisément par :
  - Système d'exploitation
    SunOS 4, AIX 4, 5, Solaris 2.6, 2.7, 2.9, RedHat 6, 7, Debian 2.2, 3.0, OpenBSD 3.3, 3.4, etc.
  - Logiciel
    iPlanet, Apache 1.3, 2, IIS 4, 5, 6, etc.
  - Equipement
    Routeurs Cisco 36xx, Nortell 2430, 5430
- Couvre des éléments de configuration ou de vérification concrets

```
echo "0" > /proc/sys/net/ipv4/ip_forward
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
```
Linux procfs

```
net.inet.ip.forwarding=0
vm.swapencrypt.enable=1
```
(Open)BSD sysctl(.conf)

Face au cycle de vie d'un projet

- Besoin détaillé ? ↔ Prendre en compte la PSSI
- Étude ? ↔ Spécifications sécurité
- Appel d'offres ↔ Spécifications sécurité
- Développement
- Intégration
- Validation ↔ Configuration / Contrôle sécurité
- Exploitation ↔ Suivi / Surveillance
- Maintenance
- Démantèlement ? ↔ Quid ?

Petit tuyau: www.dban.org
(Darik's Boot And Nuke)

Positionnement par rapport aux différents projets des entreprises

- Projets SSI
  - Associés à l'infrastructure de sécurité elle-même
  - Jonction avec les autres projets d'infrastructure
- Assistance aux projets
  - Apporter des compétences
  - Intégrer la démarche sécurité aux projets
  - Clauses contractuelles
- Validation et contrôle des projets
  - Identifier des vulnérabilités et des risques résiduels
  - Accorder des autorisations d'ouverture

Veille, Suivi

- Veille technologique
  - Alertes CERT (cf ci-avant)
  - Alertes des constructeurs
  - Nouvelles vulnérabilités
  - Nouvelles techniques de protection
- Suivi de la sécurité
  - Contrôles réguliers des vulnérabilités
  - Suivi des préconisations
  - Validation de certaines configurations (e.g.: présence des antivirus)

Synthèse – Tableau de bord

- Rendre compte
  - de la mise en place des règles
  - de l’efficacité des mécanismes de sécurité (et de leur rentabilité)
  - du niveau de vulnérabilité et de risque
  - des agressions
- Évaluer le niveau de maturité

Plan (1/2)

- Généralités
  - Propriétés de sécurité
  - Attaques
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - Suivi des alertes de sécurité
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - **Cryptographie**
  - Politiques de sécurité formelles
  - Critères d'évaluation normalisés

Terminologie

- Cryptologie = cryptographie + cryptanalyse
  - Cryptographie (κρυπτος = caché) :
    écrire des messages incompréhensibles par des tiers
  - Cryptanalyse : découvrir le(s) secret(s), décrypter

- A ne pas confondre avec stéganographie
  (στεγανος = couvert) → encre sympathique
  filigranes (tatouages)

- Chiffre, chiffrement (pas chiffrage, ni cryptage), déchiffrement, clair, cryptogramme

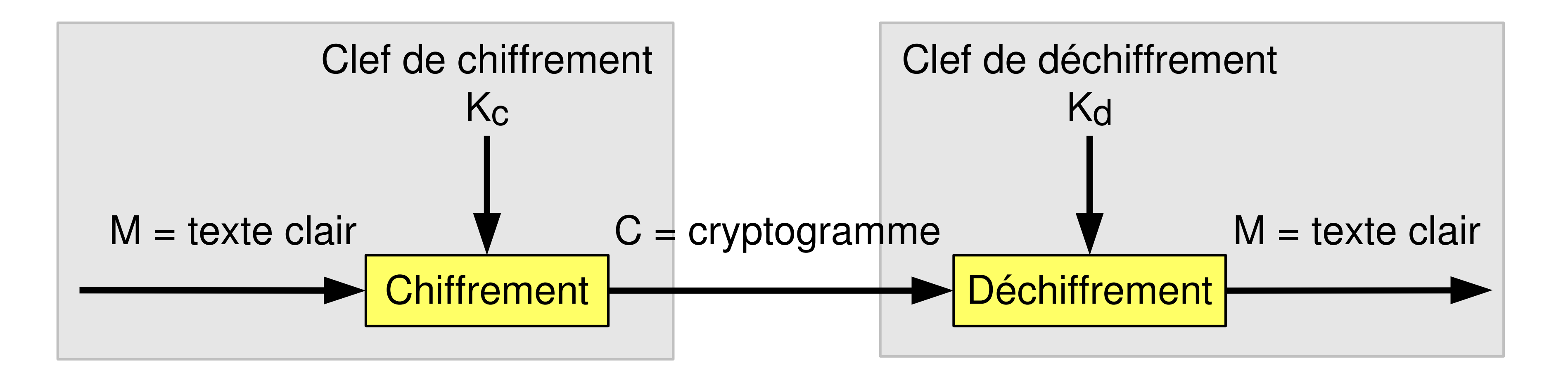
Préambule (1/2)

- C'est un des domaines des mathématiques qui a connu les avancées les plus considérables de la fin du 20ème siècle
  - Il y a rarement des preuves mathématiques générales (de solidité) dans ce domaine
  - Les chiffres se cassent
  - L'implémentation est très délicate, elle casse aussi
  - Il y a peu d'experts et même sans doute de connaisseurs
- C'est difficile et souvent contre-intuitif
  - exemple: chiffrer deux fois peut être dangereux

Préambule (2/2)

- La levée de la main-mise des militaires sur ce domaine est récente et non-vérifiable
- Les difficultés théoriques sont doublées de difficultés réelles d'implémentation
  - exemple: générateurs aléatoires, génération des clefs, protection des clefs, remplissage des blocs vides, etc.
  - notamment au niveau de la mise en oeuvre matérielle

Chiffrement (confidentialité)



- Notation chiffrement $C = \{M\}_{Kc}$
  déchiffrement $M = [C]_{Kd}$
- Confidentialité
  - Sans connaître Kd, il doit être « impossible » de retrouver M
  - Il doit être « impossible » de trouver Kd, même connaissant C et M (attaque par « clair connu »)
  - Il doit être « impossible » de trouver Kd, même connaissant C en choisissant M (attaque par « clair choisi »)

Chiffres symétriques $K_c = K_d$ (= K)

- Tous les chiffres connus jusqu'en 1976 !
- Exemples
  - DES (1976)
    - clefs de 56 bits (+8 bits de parité)
    - blocs de 64 bits
  - AES (2000)
    - clefs de 128, 192 et 256 bits
    - blocs de 128 bits

Chiffres à clef publique $K_c \neq K_d$

- Connaissant Kc, il est «impossible» de trouver Kd
  - Kd est privé (seul celui qui connaît Kd peut déchiffrer)
  - Kc est public (tout le monde peut chiffrer): répertoire de clés publiques
- Ex.: RSA (1976)
  - Appuyé (probablement) sur le problème de la factorisation des grands nombres

  $e \cdot d \equiv 1 \bmod((p-1)(q-1))$ $K_c = \{pq, e\}$ $K_d = \{p, q, d\}$
- Ex.: El Gamal (1985)
  - Basé sur la difficulté du calcul du logarithme discret dans un champs fini
  - $y = g^x \bmod p$ $K_c = \{x\}$ $K_d = \{y, g, p\}$

ou-exclusif : un chiffre embarrassant

- $C = M \oplus K$ et $M = C \oplus K$
- Aucune sécurité
  - Calculer $C \oplus C_{\gg k}$ pour $k = \{ 1, 2, ... \}$ et compter les octets identiques. L'indice de coincidence indique la longueur de la clef *n* (en octets).
  - $C \oplus C_{\gg n} = M \oplus M_{\gg n}$ élimine la clef.
  - On retrouve le message en exploitant les redondances du message d'origine (1,3 bit d'information par octet en anglais ASCII par exemple).
  - Cryptanalyse en quelques minutes.

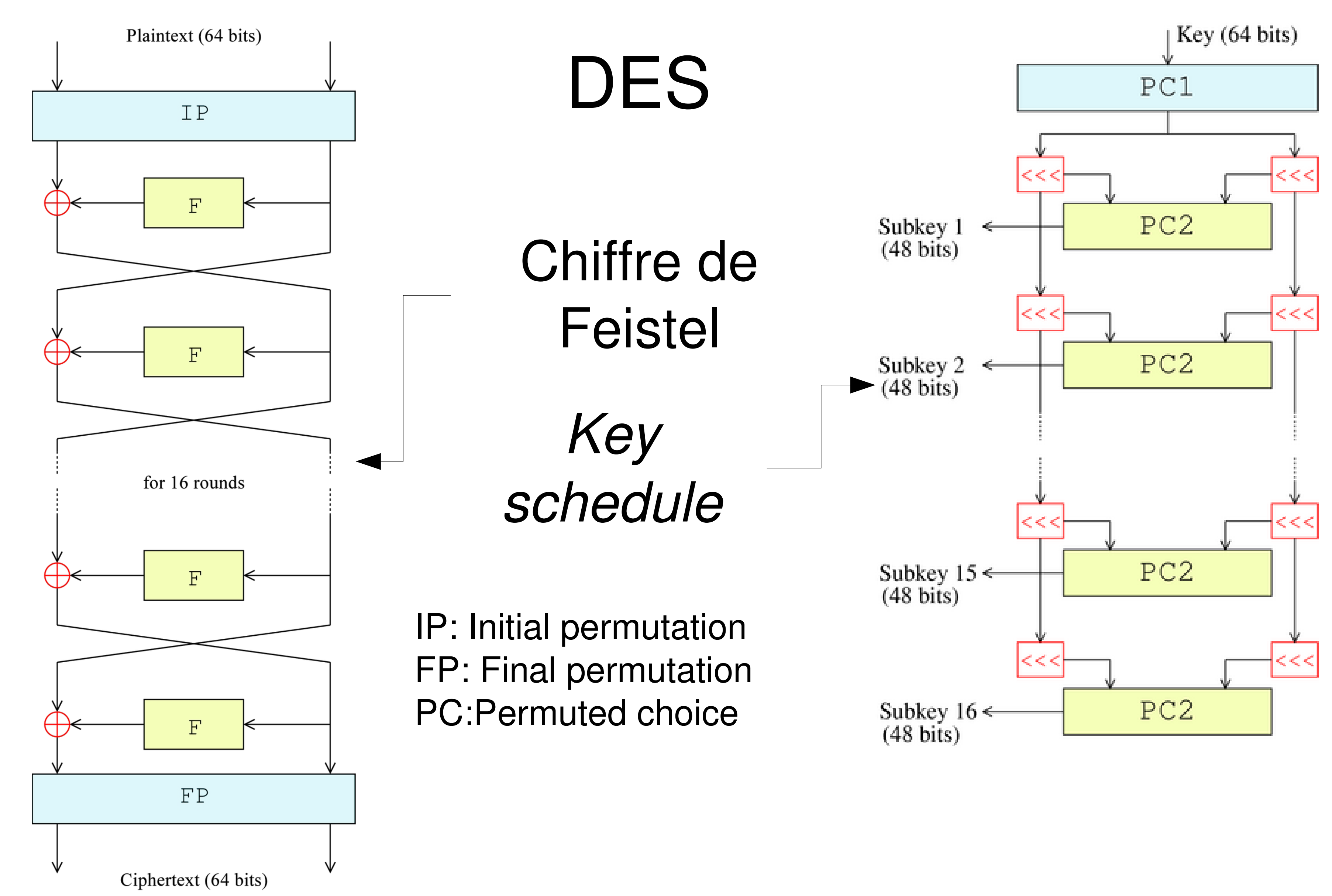
NB: C'est un chiffre polyalphabétique de Vigenère (1523-1596)

One-time pad : un chiffre parfait

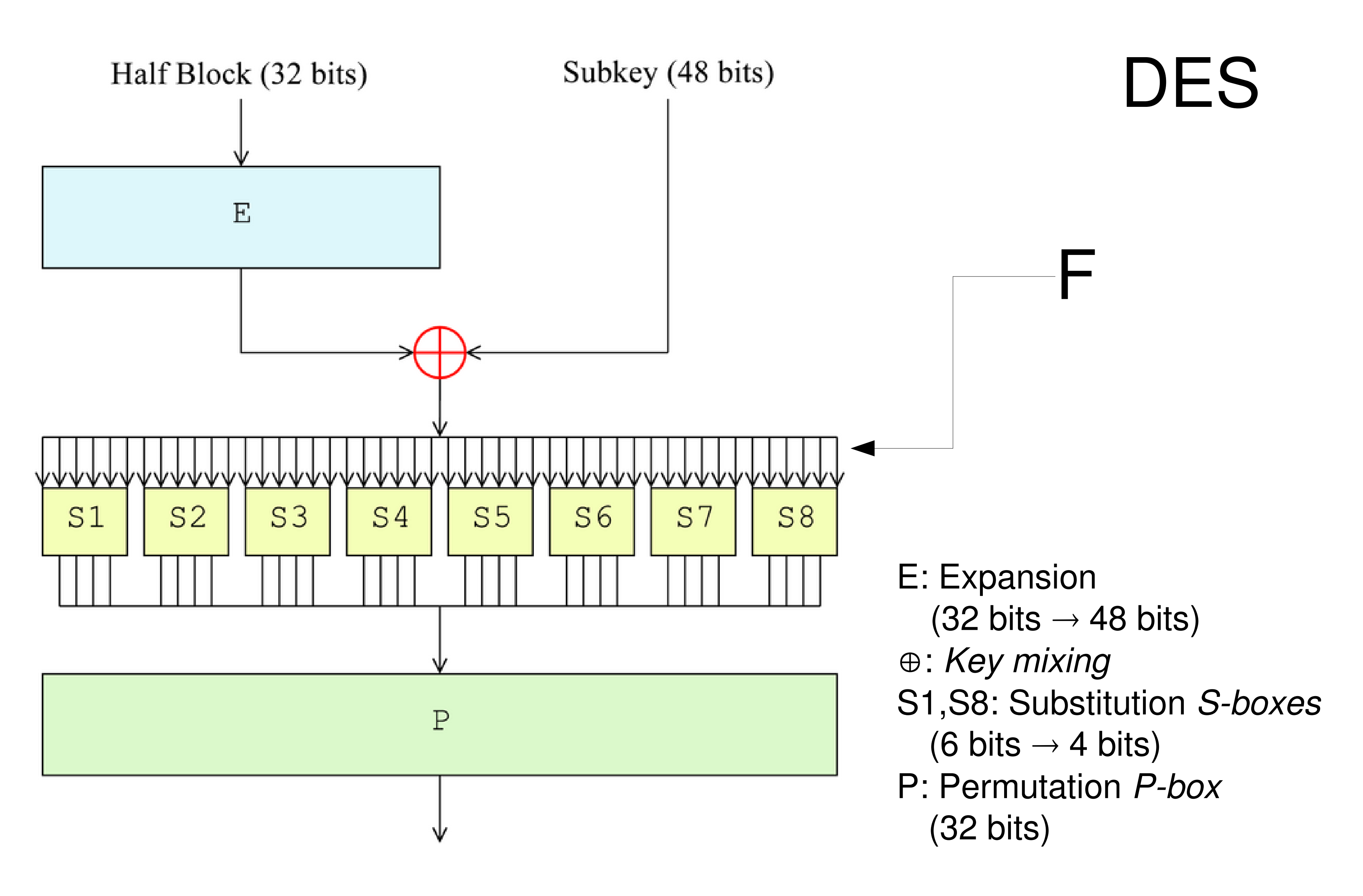
- La clef est une suite de bits aléatoire aussi longue que le message et l'algorithme est le ou-exclusif
  - $C_i = \{M_i\}_{K_i} = M_i \oplus K_i$
  - $M_i = [C_i]_{K_i} = C_i \oplus K_i$
- D'après la théorie de l'information (Shannon), c'est un chiffre incassable (si la clef n'est **jamais** réutilisée)
  - Peu pratique
  - Envisageable

DES : Data Encryption Standard (1975)

- Historique
  - Une base issue d'IBM. Des améliorations de la NSA.
  - Le premier algorithme controlé par la NSA rendu public... par l'organisme de standardisation.
- Bloc de 64 bits. Clef de 56 bits + 8 bits (ex.: parité)
- Conception orientée vers une mise en œuvre *hardware*
- 3DES : amélioration (générique) répandue
  - clef de 112 bits
- Énormes efforts publics de cryptologie
- Beaucoup de variantes (ex.: *key-dependent S-boxes*)



http://en.wikipedia.org/wiki/Data_Encryption_Standard


Half Block (32 bits)
Subkey (48 bits)
DES
E
F
S1
S2
S3
S4
S5
S6
S7
S8
P
E: Expansion
(32 bits → 48 bits)
⊕: *Key mixing*
S1,S8: Substitution *S-boxes*
(6 bits → 4 bits)
P: Permutation *P-box*
(32 bits)

DES

Electronic Frontier
Foundation
DES Cracker
“Deep Crack”
~5 jours



Modes de fonctionnement des chiffres symétriques

$M = M_1 \cdot M_2 \cdot \ldots \cdot M_n$ $C = C_1 \cdot C_2 \cdot \ldots \cdot C_n$

- ECB – *Electronic Codebook*
  - $C_i = \{M_i\}_K$
  - $M_i = [C_i]_K$
- CBC – *Cipher Block Chaining*
  - $C_i = \{M_i \oplus C_{i-1}\}_K$
  - $M_i = C_{i-1} \oplus [C_i]_K$
  - IV sorte de M_0
- Stream ciphers
  - CFB – Cipher Feedback Mode
  - OFB – Output Feedback Mode

Avantages des chiffres symétriques

- Rapides
  - ~1 Gb/s par hard
  - ~100 Mb/s par soft
- Clefs « courtes »
  - typiquement 80 bits pour résister aux attaques brutales (aujourd'hui)
- Pratiques pour chiffrer des fichiers personnels (pas de clef à partager)

Problèmes des chiffres symétriques

- En communication, la clef secrète est partagée
  - l'émetteur et le récepteur doivent se faire confiance, et garder soigneusement la clef secrète
- Comment distribuer ou renouveler la clé ?
  - Chiffrer la nouvelle clé de session avec l'ancienne
  - Chiffrer la clé de session avec une clé spécifique de chaque matériel $\Rightarrow$ site de confiance (répertoire)
  - Utiliser un système à clé publique (Diffie-Hellmann)
  - Crypto. quantique
  - Pigeon voyageur

RSA

- Clef publique
  - n : produit de deux (grands) nombres premiers p et q (p et q doivent rester secrets)
  - e : premier avec (p-1)(q-1)
- Clef privée
  - d : $e^{-1} \bmod ((p-1)(q-1))$
- Chiffrement
  - $c = m^e \bmod n$
- Déchiffrement
  - $m = c^d \bmod n$

El Gamal (signature)

- Clef publique
  - p : premier
  - $g < p$
  - $y = g^x \bmod p$
- Clef privée
  - $x < p$
- Signature
  - k : choisi au hasard, premier avec p-1
  - (a,b) : $a = g^k \bmod p$ et $M = (xa + kb) \bmod (p-1)$
- Vérification
  - Valide si $y^a a^b \bmod p = g^M \bmod p$

El Gamal (chiffrement)

- Clef publique
  - p : premier
  - $g < p$
  - $y = g^x \bmod p$
- Clef privée
  - $x < p$
- Chiffrement
  - k : choisi au hasard, premier avec p-1
  - C=(a,b) : $a = g^k \bmod p$ et $b = y^k M \bmod p$
- Déchiffrement
  - $M = b / a^x \bmod p$

Avantages des chiffres à clef publique

- Pas de confiance mutuelle entre émetteur et récepteur

- Gestion de clé « facile »
  - Répertoire public de clés publiques ou distribution entre pairs
  - La clé privée ne doit « jamais » être transmise

- Permettent des utilisations nouvelles : distribution de clés symétriques, signatures, certificats, …

Échange de clefs symétriques

- Exemple : Alice génère aléatoirement une clé de session K (symétrique) et la chiffre avec la clé publique de Bob

- Exemple : Diffie-Hellmann

  Alice génère aléatoirement :

  n : grand nombre premier tel que $(n-1)/2$ soit aussi premier

  et choisit g = générateur d'un sous-groupe q de n

  (typiquement, $g = 2$, $q = (n-1)/2$)

  x (clé secrète d'Alice) est tel que $\log_g n < x < q$

  1. Alice calcule $K_a = g^x \bmod n$ et transmet (n, g, K_a) à Bob.
  2. Bob génère aléatoirement y (clé secrète de Bob),
     calcule $K_b = g^y \bmod n$, et transmet K_b à Alice.
  3. Alice et Bob peuvent alors calculer séparément une clé de session
     $K = {K_b}^x \bmod n = {K_a}^y \bmod n = g^{xy} \bmod n$

Inconvénients des chiffres à clef publique

- Calculs complexes
  - lents ($\sim$1 Mb/s)
  - clef longue (1024 ou 2048 bits), sauf avec des courbes elliptiques ($\sim$160 bits)

- Problèmes spécifiques
  - Intégrité des répertoires de clés publiques
  - Durée de vie des clés
  - Révocation
  - Nécessité de partager des clés privées ?
  - Limitation des algorithmes : ex. chiffrer un petit M par RSA

Fonctions de hachage → empreinte

- « One-way hash function » H
  - L'empreinte H(M) est de taille fixe n (ex: 128 bits) quelle que soit la longueur de M
  - La probabilité que 2 messages différents M et M' aient la même empreinte H(M)=H(M') est $\sim 1/2^n$
  - Connaissant M, il est facile de calculer H(M)
  - Connaissant M, il est impossible de trouver $M' \neq M$ tel que H(M') = H(M)
- Exemples: MD5, SHA-1, SHA-256, DES en mode CBC
- Typiquement, on découpe M en blocs $m_1, m_2, ..., m_k$
  $h_1=F(cte,m_1)$, $h_2 = F(h_1,m_2)$, ..., $h_k = F(h_{k-1},m_k) = H(M)$

Application : intégrité

- Communications : contre interception et modification transmettre le message et l'empreinte par des canaux indépendants
- Fichiers : détection de modifications
  - Exemples : Tripwire, Samhain
  - Sur une machine de confiance, calculer les empreintes des fichiers stables (OS, programmes, configuration, ...) et les stocker de manière protégée
  - Périodiquement ou en cas de doute, recalculer les empreintes et les comparer (sur une machine de confiance)

Signature (intégrité)

- Ks = clef de signature ; Kv = clef de vérification
- Signatures symétriques Ks = Kv
  - Exemple: dernier bloc DES-CBC
  - Signataire et vérificateur doivent se faire confiance
  - La signature n'est pas valable devant un juge
- Signatures asymétriques Ks ≠ Kv
  - Hachage puis chiffrement empreinte: Ks=Kc, Kv=Kd
  - Vérifiable par des tiers

    Il faut être sûr de ce que l'on signe !
  - Peuvent servir à sécuriser les répertoires de clefs publiques
    - Chaque entrée du répertoire est signée par une autorité (de certification).
    - Les clés des AC sont structurées dans un répertoire en arbre

L'époque contemporaine

- 2004
  - Il y a de sérieux doutes théoriques sur MD5 (classes de collisions)
  - Il y a des possibilités d'extrapolation sur SHA-1
- 2005
  - MD5 n'est plus considérée de confiance
  - Il y a des doutes théoriques sur SHA-1 (collisions en nombre)
- 2006
  - Des rumeurs entourent SHA-1 (« les calculs sont en cours »)
- 2007-11-02 NIST *hash function competition* (SHA-3)
- 2010-12-10 : 5 finalistes

Julius. Caesar
Via Appia 1
Rome, The Roman Empire

May, 22, 2005

To Whom it May Concern:

Alice Falbala fulfilled all the requirements of the Roman Empire intern position. She was excellent at translating roman into her gaul native language, learned very rapidly, and worked with considerable independence and confidence.

Her basic work habits such as punctuality, interpersonal deportment, communication skills, and completing assigned and self-determined goals were all excellent.

I recommend Alice for challenging positions in which creativity, reliability, and language skills are required.

I highly recommend hiring her. If you'd like to discuss her attributes in more detail, please don't hesitate to contact me.

Sincerely,

Julius Caesar

Julius. Caesar
Via Appia 1
Rome, The Roman Empire

May, 22, 2005

Order:

Alice Falbala is given full access to all confidential and secret information about GAUL.

Sincerely,

Julius Caesar

http://www.cits.rub.de/**MD5Collisions**/

```
ortalo@hurricane:~/$ md5sum letter_of_rec.ps order.ps
a25f7f0b29ee0b3968c860738533a4b9  letter_of_rec.ps
a25f7f0b29ee0b3968c860738533a4b9  order.ps
ortalo@hurricane:~/$
```

Schémas à seuil

- Stocker K sous la forme d'un ensemble de valeurs Ki (images) telles que
  - S images permettent de reconstruire le secret (S est le seuil)
  - S-1 images n'apportent aucune information
- Si on sait générer N images (avec N>S), alors on tolère de perdre jusqu'à N-S images
- Exemple d'idée
  - Si l'on connait S=n+1 point d'un polynôme P de degré n, on sait recalculer les coefficients a_n du polynôme
    (n+1 équations à n+1 inconnues)
  - Passer dans un corps de Galois (modulo q avec q premier)

Autres sujets (non-abordés)

- Stéganographie
- *Watermarking* (tatouage)
- Générateurs aléatoires
- Génération de nombres premiers
- Écrous (key escrow)
- Vote
- Horodatage
- Destruction
- Protocoles
- Cryptanalyse

Overall presentation (1/2)

- Fast paced computer security walkthrough
  - Security properties
  - Attacks categories
  - Elements of cryptography
  - Introduction to mandatory security policies
- Embedded systems and security
  - Specificities
  - Physical attacks (SPA, DPA)
  - TPM
- **Software development and security**
  - **Security requirements and process**
  - Static verification and software development tools
  - Common criteria / ISO 15408

Problem to address (with respect to security requirements definition)

- Best ROI when done at application design phase
- When considered at all, they tend to be
  - general lists of security features
    - password, firewalls, antivirus, etc.
  - implementation mechanisms ≠ security requirements
  - intented to satisfy *unstated* requirements
    - authenticated access, etc.
- Exist in a section by themselves (copied from a generic set)
  - no elicitation or analysis process, no adaptation to the target
- Significant attention is given to what the system should do
  - little is given to what it should not do *(in req. eng.)*
- Priority is not given to security (wrt ease of use for example)

Note on security updates

- How can we manage software vulnerabilities?
  - Wait until they are exploited by an attacker
  - Quickly provide a patch that should correct the problem (without introducing another one)
  - Whine because system administrators do not install patches fast enough

- Astonishingly it is very popular
  - All serious editors do that
  - Users feel more secure (still?)

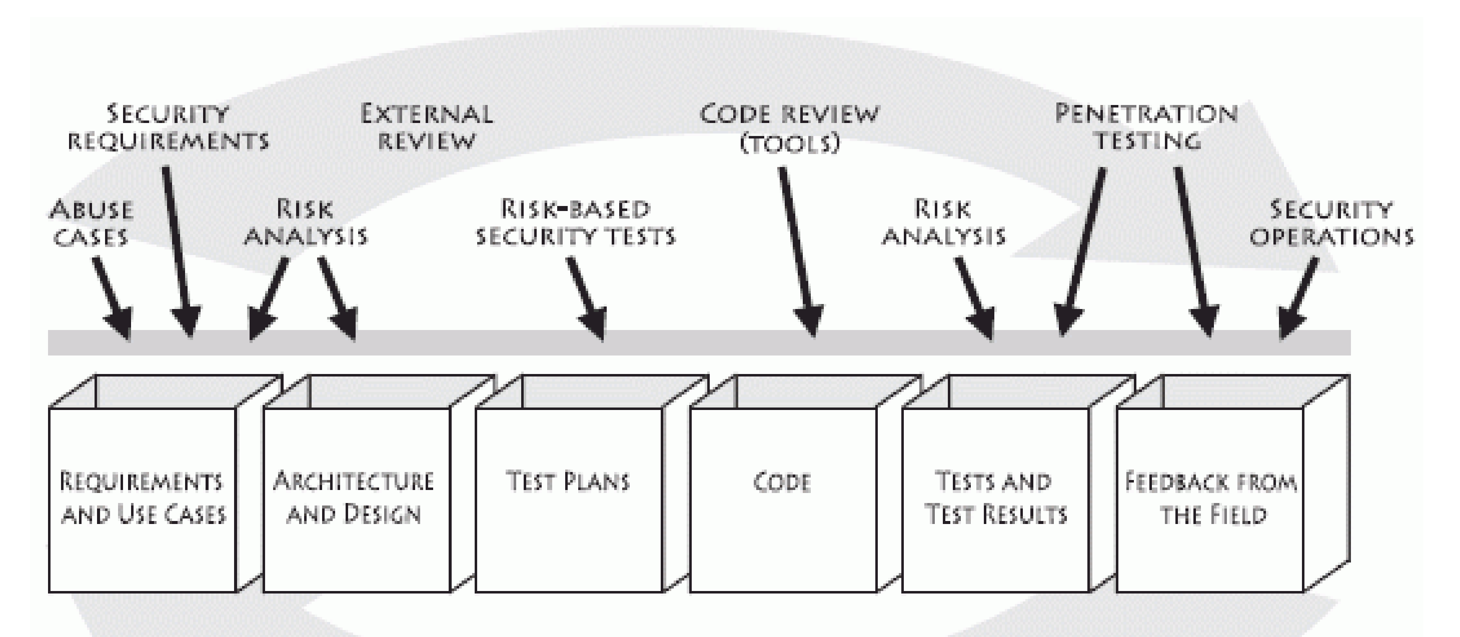
Improving security Using Extensible Lightweight Static Analysis, David Evans and David Larochelle, *IEEE Software*, January/February 2002.

In other words

- It is not enough to apply patches to secure a system
- Also, you cannot rely only on firewalls or antivirus (or IT security tools)
- Security objectives of a piece of software should be identified
- Security implies a change in point of view
  - e.g.: it must *not* work
  - unavailable is better than destroyed
  - which (computer) is saved first ?

Another view on project lifecycle

- Detailed needs ? ⟷ Security policy consideration
- Specs ? ⟷ Security specification
- Contracts ⟷ Security specification
- Development
- Integration
- Validation ⟷ Security validation/configuration
- Exploitation ⟷ Monitoring / Management
- Maintenance ⟷ Quid ?
- Disposal ?



1. Code review
2. Architectural risk analysis
3. Penetration testing
4. Risk-based security tests
5. Abuse cases
6. Security requirements
7. Security operations

Gary McGraw's Touchpoints

Risk analysis

1. Identify assets and their value ($$)
2. Define assets priority
3. Identify vulnerabilities, threats and potential damages
4. Define threats priority
5. Optimize counter-measures selection

- Inherently qualitative (human/expert opinion)
- Applicable to organization, system, project
- Several methods available
  - MARION, MEHARI, EBIOS, etc.
  - HAZOP, FMEA, ISO31000, etc.

Pros (my view)

- *Identification* of assets and their relative values
- Assets value offers an opportunity to budget realistically (for protection)
- Is understandable by end users
  - Quite easier than assembly language exploits or cryptographic hash functions
- Risk management alternatives
  - Transfer (insurance, state, etc.)
  - Acceptance (life is deadly after all)
  - Reduction (work, work, work, work, ...)
  - Avoidance (just do it the other way)
- Management could express clear priorities

Cons (my view)

- Threat determination is an oracle problem
- May be used to demonstrate that (any) risk is (already) managed
  - Some forgotten successes of risk management
    - Lehman-Brothers financial risk exposure
    - Greek debt control
  - Qualitative also means manipulable
- Relies a lot on best practices or risks lists
  - Fuels paranoia and ready-made useless tools
  - Does not help target real assets
- Management rarely wants to decide
- Sometimes does not end well morally speaking
  - For example : product lifetime optimization
  - (NB : Inherently viewpoint-based)

Threats and use-case examples

- Trusted Computing Group
  - Mobile phone TPM use-case scenarios
  - *(Name,) Goal*
    - *Threats*

- Platform integrity
  - Ensure that device possess and run only authorized operating system(s) and hardware
    - Logic of device firmware modified
    - Device hardware modified
    - Device functions in a manner other than intended by the manufacturer
    - Device modified to broadcast false identification (IMEI)

Threats and goals examples

- Device authentication
  - Assist user authentication
  - Prove identity of device itself
    - Identity spoofing to get unauthorized access to services
    - Identity no longer bound to the device
    - Theft of device
    - Device tracking
- Robust DRM implementation
  - Service and content providers need assurance that the device DRM is robust
- SIMLock / Device personalisation
  - Ensure that a mobile device remains locked on a particular network

Last use-case examples (for info.)

- Secure software download
- Secure channel between device and UICC (UMTS Integrated Circuit Card)
- Mobile Ticketing
- Mobile Payment
- Software use
  - User-available predefined software use policies
- Proving platform and/or application integrity to end user
- User data protection and privacy

Not a use-case but...

- An interesting idea
  - *Cloaking Malware with the Trusted Platform Module*, A. Dunn, O. Hofmann, B. Waters, E. Witchel, University of Texas at Austin.
  - Use the TPM to hide the payload (ie. the target) of a malicious software
  - Provide a way to counter malware analysis
- Sort of « Secure software download » but for the bad guys
- Remember that, today, attackers usually know computer security better than you do

References

- DHS « Build Security In »
  - https://buildsecurityin.us-cert.gov/
- The Addison-Wesley Software Security Series
  - http://www.softwaresecurityengineering.com/series/
- CERT/CC
  - http://www.cert.org/
- « *Smashing the Stack for Fun and Profit.* »
  - Aleph One, Phrack Magazine 7, 49 (1996)
    File 14 of 16.
- OpenBSD
  - http://www.openbsd.org/papers/

Some real programming

- Presentation based on work from real programmers in the neighbourhood
- First, sources :
  - Matthieu Herrb & lots of OpenBSD « good programming » examples
  - Vincent Nicomette and Eric Alata for some « details »

Now real programming (*prereq.*)

```
#include <stdio.h>
void copie(char * s) {
  char ch[8] = "BBBBBBBB" ;
  strcpy(ch,s) ;
}
int main(int argc, char * argv[]) {
  copie(argv[1]) ;
  return(0);
}
```

AAAAAAAAAAAA[system_adr][exit_adr][shlibc_adr]

Bash$./a.out 'perl -e 'print "A"x12 . 0xb7ee1990 . 0xb7ed72e0 . 0xb7fcc0af' '

sh-3.1$

Now real programming

- Number One : buffer overflow with string functions

```
strcpy(path, getenv("$HOME"));
strcat(path, "/");
strcat(path, ".foorc");
len = strlen(path);
```

- strcat(), strcpy()
  - no verification on buffer size, dangerous : do not use
- strncat(), strncpy()
  - leave strings non terminated, very difficult to use correctly
- strlcat(), strlcpy()
  - May truncate strings, but probably easier to use

http://homepages.laas.fr/matthieu/cours/mh-prog-defensive.pdf

str{,n,l}{cpy,cat} practical usage

```
STRCAT(3)                  Linux Programmer's Manual                  STRCAT(3)

NAME
       strcat, strncat - concatenate two strings

SYNOPSIS
       #include <string.h>

       char *strcat(char *dest, const char *src);

       char *strncat(char *dest, const char *src, size_t n);
```

No strlcat() on Linux ; so, from the BSDs (more precisely OpenBSD) :

```
size_t strlcpy(char *dst, const char *src, size_t dstsize);
size_t strlcat(char *dst, const char *src, size_t dstsize);
```

strncat() is difficult to use

```
strncpy(path, homedir, sizeof(path) – 1) ;
path[sizeof(path) – 1] = '\0' ;
strncat(path, "/", sizeof(path) – strlen(path) – 1) ;
strncat(path, ".foorc", sizeof(path) – strlen(path)
    – 1) ;
len = strlen(path) ;
```

Note (on Linux) : g_strlcpy() and g_strlcat() exist in glib-2.0

Note (on BSD) : see next slide (*Yeah !!!)*

Additional note: C11 has removed gets() (was deprecated in C99) replaced by ***gets_s()***

strl*() look better

```
strlcpy(path, homedir, sizeof(path)) ;
strlcat(path, "/", sizeof(path)) ;
strlcat(path, ".foorc", sizeof(path)) ;
len = strlen(path) ;
```

- May truncate, but no overflow

- Add checks for non testing code :

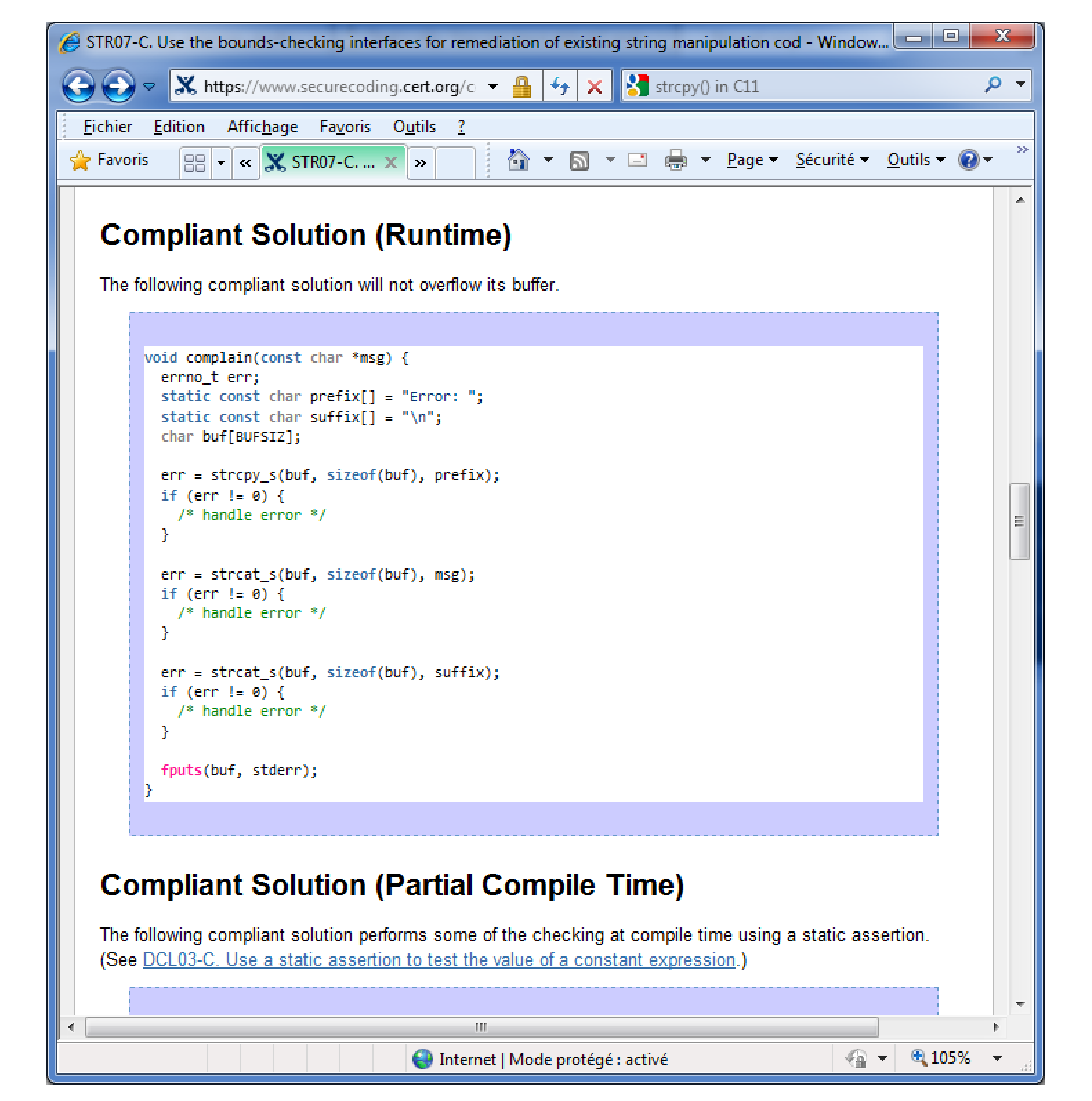
```
strlcpy(path, homedir, sizeof(path)) ;
if (len >= sizeof(path)) return (ENAMETOOLONG) ;
strlcat(path, "/", sizeof(path)) ;
if (len >= sizeof(path)) return (ENAMETOOLONG) ;
strlcat(path, ".foorc", sizeof(path)) ;
if (len >= sizeof(path)) return (ENAMETOOLONG) ;
len = strlen(path) ;
```

C11 Annex K (ISO/IEC 9899:2011)

- C11 Ann.K « Bounds-checking interfaces » defines alternative versions of standard string-handling functions (from Microsoft)
- strcpy_s(), strcat_s(), strncpy_s() and strncat_s()
- *ie* :

```
errno_t strcpy_s(
char * restrict s1,
rsize_t s1max,
const char * restrict s2
);
```

- See also : ISO/IEC TR24731-1:1999 and ISO/IEC:TR24731-2:2010 …
- Note : wchar_t



Compliant Solution (Runtime)

The following compliant solution will not overflow its buffer.

```
void complain(const char *msg) {
  errno_t err;
  static const char prefix[] = "Error: ";
  static const char suffix[] = "\n";
  char buf[BUFSIZ];

  err = strcpy_s(buf, sizeof(buf), prefix);
  if (err != 0) {
    /* handle error */
  }

  err = strcat_s(buf, sizeof(buf), msg);
  if (err != 0) {
    /* handle error */
  }

  err = strcat_s(buf, sizeof(buf), suffix);
  if (err != 0) {
    /* handle error */
  }

  fputs(buf, stderr);
}
```

Compliant Solution (Partial Compile Time)

The following compliant solution performs some of the checking at compile time using a static assertion. (See DCL03-C. Use a static assertion to test the value of a constant expression.)

Raw C11 example
from https://www.securecoding.cert.org/

Time of check, time of use

- How to create a temp. file in /tmp without overwriting an existing file ?

```
/* Generate random file name */
name = mktemp("/tmp/tmp.XXXXXXXXXX");
/* verify file does not exist */
if (stat(name,&statbuf) == 0) {
    return EEXISTS;
}
/* ok, open it */
fd = open(name, O_RDWR);
```

- Opens a possible race condition with a concurrent process
- mktemp() deprecated in POSIX.1 (2011)

Options

- Use mkstemp() to replace both system calls
```
fd = mkstemp("/tmp/tmp.XXXXXXXXXX") ;
```
- Use O_CREAT | O_EXCL, open() flags that trigger an error if the file already exists
```
fd = open(name, O_CREAT | O_EXCL);
```
- Note the difference between fopen() and open() return types (FILE* vs. int or streams vs. file descriptors)

Arithmetic overflows

```
n = getIntFromUser();
if (n<=0 || n*sizeof(struct item) > BUFMAX){
    return EINVAL;
}
```

- If *n* is big enough, the condition will not be true
- Use :

```
n = getIntFromUser();
if (n<=0 || n > BUFMAX/sizeof(struct item)){
    return EINVAL;
}
```

Arithmetic overflows

```
n = getIntFromUser();
if (n<=0){
    return EINVAL;
}
data = (struct item *)
    malloc(n * sizeof(struct item));
if (data == NULL) {
    return ENOMEM;
}
```

- If *n* is big enough, overflow occurs and a small memory allocation is done
  - opening the path to a memory overflow
- Use calloc() !

```
data = (struct item *)
    calloc(n, sizeof(struct item));
```

Format strings issues

- Many standard display functions use a format for printing : printf(), sprintf(), fprintf(), …
- Two variants exist, with and without format strings : printf("%s", ch) or printf(ch)
- What happens when you give « %x » to printf ?
  - printf() gets its next argument from the stack
- When user input is passed to such functions, it can generate this kind of situations
- This kind of situation may allow to access areas of memory for reading (sometimes for writing)

Example

```
#include <stdio.h>
int main()
{
    char * secret = "polichinelle";
    static char input[100] = {0};
    Printf("Enter your name: ");
    scanf("%s", input);
    printf("Hello ");printf(input);printf("\n");
    printf("Enter your password: ");
    scanf("%s",input);
    if (strcmp(entree,secret)==0) {
        printf("OK\n");
    } else {
        printf("Error\n");
    }
    return 0;
}
```

Example

- Normal use of the program

```
bash$ ./a.out
Enter your name: Jack
Hello Jack
Enter your password: ripper
Error
```

- « Abuse » of the program

```
bash$ ./a.out
Enter your name: %p%s
Hello 0x08049760polichinelle
```

- Allows to walk the stack and access internal program data

Practical recommendations

- Design first
  - Often broken and insecure by design
- Obscurity does not help
  - Exploits against closed source may be just as easy as against open source
  - Obfuscation primarily works for people writing code, not crackers
- Quality is security
  - Most security problems are simple bugs
  - There is no security plugin
  - No ROI for security
    - But shorter test cycles
    - Less bugs, so less time spent fixing them
    - And usually better efficiency

Practical recommendations

- Most code should be simple and boring
  - Easier to audit
  - Already formatted
  - Clever code is almost always wrong
- Fix a bug everywhere
  - Even automate for checking it
- Check return codes
- Design your APIs right...
- Understand semantics
  - File descriptors
    - Inheritance over fork
    - Access rights only checked on open()
  - Signal handlers *are* complex
    - Simple rule : only set volatile atomic flags in them

Practical recommendations

- Most security issues come from abstraction layers violation (audit these cases)
  - Hidden variables
  - Concurrency
  - Overflows
  - Flow control on error
- All user input must be checked
  - Positive checks
  - Everything not static is like user input
- Be careful with optimizations

- There is no secure language or environment
  - Java does not suffer from simple buffer overflows but has integer overflows, logic errors, etc.

Exemples de patch/bug

- Origine : OpenBSD (2006, 2007)
- Correction du serveur httpd (patch)
  - Absence de nettoyage d'un header HTTP (Expect:)
  - Possibilité de XSS
  - CVE-2006-3918
- Correction de ld.so (patch)
  - Nettoyage de l'environnement
  - Exploitable ?
- Correction de la commande file (patch)
  - Débordement de pile
  - CVE-2007-1536

Exemples d'attaques

- Essais répétitifs (*brute force*) : script expect
- Interactions script système et bug (patch) : programme C
- Programme Windows (injection DLL)
- Fichier image

http://www.determina.com/security.research/vulnerabilities/ani-header.html

Curseur ANImé sous Windows (1/3)

CVE-2007-0038 (CVE-2005-0416 bis)

```
struct ANIChunk
{
    char  tag[4];          // ASCII tag
    DWORD size;            // length of data in bytes
    char  data[size];      // variable sized data
}

int LoadCursorIconFromFileMap(struct MappedFile* file, ...)
{
    struct ANIChunk  chunk;
    struct ANIHeader header;        // 36 byte structure
    ...
    // read the first 8 bytes of the chunk
    ReadTag(file, &chunk);

    if (chunk.tag == 'anih') {

+       if (chunk.size != 36)       // added in MS05-002
+           return 0;

        // read chunk.size bytes of data into the header struct
        ReadChunk(file, &chunk, &header);
```

Curseur ANImé sous Windows (2/3)

CVE-2007-0038 (CVE-2005-0416 bis)

```
int LoadAniIcon(struct MappedFile* file, ...)
{
    struct ANIChunk  chunk;
    struct ANIHeader header;        // 36 byte structure
    ...
    while (1) {
        // read the first 8 bytes of the chunk
        ReadTag(file, &chunk);
        switch (chunk.tag) {
            case 'seq ':
                ...
            case 'LIST':
                ...
            case 'rate':
                ...
            case 'anih':
                // read chunk.size bytes of data into the header
  struct
                ReadChunk(file, &chunk, &header);
```

Curseur ANImé sous Windows (3/3)

CVE-2007-0038 (CVE-2005-0416 bis)

- LoadCursorIconFromFileMap appelle LoadAniIcon
- LoadCursorIconFromFileMap ne valide que le *premier* fragment `anih`
- Un fichier .ANI :

```
00000000   52 49 46 46  90 00 00 00  41 43 4F 4E  61 6E 69 68   RIFF....ACONanih
00000010   24 00 00 00  24 00 00 00  02 00 00 00  00 00 00 00   $...$...........
00000020   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000030   00 00 00 00  01 00 00 00  61 6E 69 68  58 00 00 00   ........anihX...
00000040   41 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41   AAAAAAAAAAAAAAAA
00000050   41 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41   AAAAAAAAAAAAAAAA
00000060   00 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41   .AAAAAAAAAAAAAAA
00000070   41 41 41 41  41 41 41 41  41 41 41 41  00 00 00 00   AAAAAAAAAAAA....
00000080   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000090   42 42 42 42  43 43 43 43                             BBBBCCCC
```

- NB: Evite les protections contre les débordements du compilateur Vista (/GS) centrées sur les tableaux (et non les struct). Bug situé dans un code tolérant les exceptions

Fun with NULL pointers

- Linux 2.6.30 kernel local root exploit
- Brad Spengler
  - cheddar_bay.tgz
  - http://lwn.net/Articles/341773/
- Jonathan Corbet, LWN.net, 20&21 juillet 2009
  - Part 1 http://lwn.net/Articles/342330/
  - Part 2 http://lwn.net/Articles/342420/
- Comments from various readers

Plan (1/2)

- Généralités
  - Propriétés de sécurité
  - Attaques
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - Suivi des alertes de sécurité
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - Cryptographie
  - **Politiques de sécurité formelles**
  - Critères d'évaluation normalisés

Politiques et modèles de sécurité

- La politique de sécurité
  - « *est l'ensemble des lois, règles et pratiques qui régissent la façon dont l'information sensibles et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique*. » [ITSEC, 1991]
  - physique, administrative, logique
- Modèle de sécurité
  - Formalisme ou représentation mathématique
- Partition entre entités
  - actives: sujets s
  - passives: objets o

Politiques discrétionnaires et obligatoires

- Politique discrétionnaire
  - chaque objet *o* est associé à un sujet *s* précis, son propriétaire qui manipule les droits d'accès à sa discrétion
  - le propriétaire peut librement définir et transmettre ces droits à lui-même ou un autre utilisateur
- Politique obligatoire
  - règles discrétionnaires (droit d'accès)
  - *plus* : règles incontournables (habilitation)

Matrice de contrôle d'accès

[Lampson 1971]

- Machine à états : état = (S,O,M)
  - O ensemble d'objets
  - S ensemble de sujets ($S \subseteq O$)
  - $M(s,o)$ est l'ensemble des droits que le sujet s possède sur l'objet o
  - les droits sont pris dans un ensemble fini A

Modèle HRU (1976)

- Commandes de modification

  command $\alpha(x_1, x_2, ...x_k)$

  if $a' \in M(s',o')$ and $a'' \in M(s'',o'')$ and ... and $a^{(m)} \in M(s^{(m)},o^{(m)})$

  then op_1; op_2; ...; op_n

  end

  $a^{(i)} \in A$

  op_i: *create a into M(s,o)* — *delete a from M(s,o)*

  create subject s — *destroy subject s*

  create object o — *destroy object o*

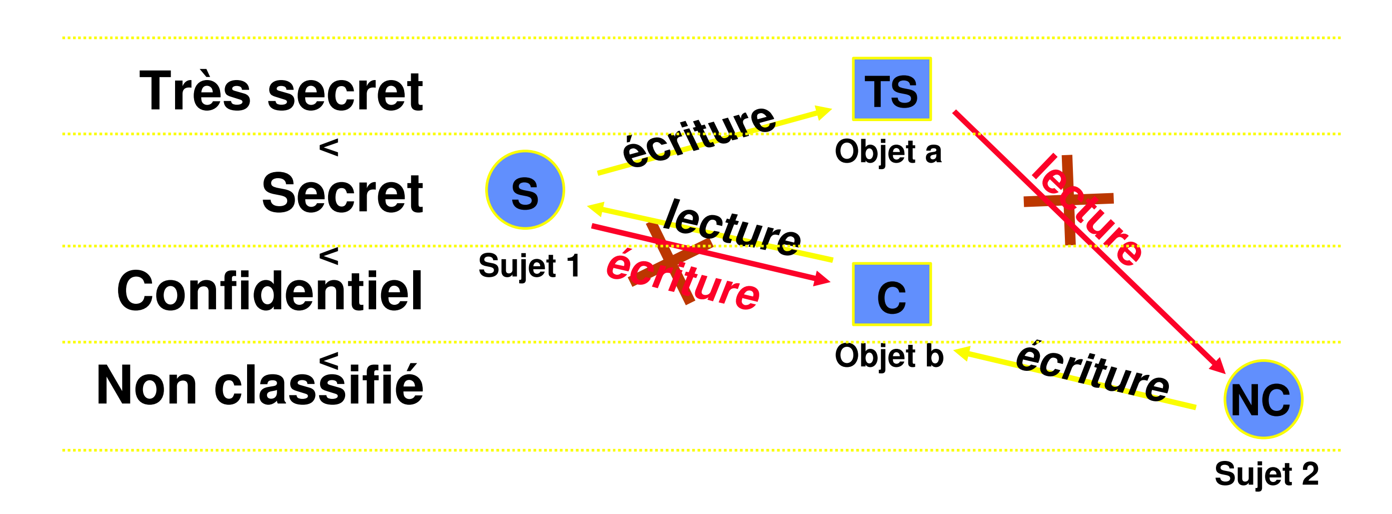
- Problème de protection (Q_0 sûr pour a)
  - *indécidable* dans le cas général
  - *décidable* pour les systèmes à mono-opération (n=1)

Autres modèles dérivés

- Take-Grant (1976)
  - algorithme de décision de complexité linéaire
- SPM et TAM (1988, 1992)
- rôles
  - RBAC (1996)

Politique multiniveau de Bell-LaPadula (1975)

- niveau (d'habilitation) des sujets *h(s)*
- niveau (de classification) des objets *c(o)*
- interdire les fuites d'information d'un objet vers un objet de niveau inférieur
- interdire à tout sujet d'obtenir des information d'un objet de niveau supérieur à son habilitation



Modèle de Bell-LaPadula

- classification *cl* : ensemble totalement ordonné
- compartiment *C* : ensemble de catégories
- $n=(cl,C)$, $n'=(cl',C')$: n n' $\Leftrightarrow$ $cl \leq cl'$ et $C \subseteq C'$ (treillis)
- propriété simple

$$\forall s \in S,\ \forall o \in O,\ \text{read} \in M(s,o) \Rightarrow c(o)\quad h(s)$$

- propriété $\star$

$$\forall s \in S,\ \forall (o,o') \in O^2,\ \text{read} \in M(s,o) \wedge \text{write} \in M(s,o') \Rightarrow c(o)\quad c(o')$$

Inconvénients de BLP et Politique de Biba

- Inconvénients
  - L'information se dégrade constamment par surclassification (ou on introduit des procédures de déclassification hors modèle)
  - Le modèle ne représente pas tous les flux d'information et ne prend pas en compte les canaux cachés
- Politique de Biba
  - duale de BLP pour assurer l'intégrité
  - droits = { modifier, observer, invoquer }
  - inconvénient similaire : le niveau d'intégrité de l'information se dégrade constamment

Politiques de contrôle d'interface – Modèle

- ensemble S de sujets, ensemble Γ de commandes ou opérations, ensemble d'états Σ du système, σ_0 état initial
- un ensemble Out dont les éléments sont les sorties visibles par un utilisateur
- out : $\Sigma \times S \rightarrow$ Out do : $\Sigma \times S \times \Gamma \rightarrow \Sigma$
- **trace**, suite ordonnée de commandes
  $w \in traces = (S \times \Gamma)^*$
- $[w] \in \Sigma$ état atteint en partant de σ_0
- $\langle\ \rangle$, $\nu \cdot \gamma_1(u_1) \cdot \gamma_2(u_2) \cdot \ldots \cdot \gamma_n(u_n)$, $(\gamma_i)_{1 \leq i \leq n}$, $(u_i)_{1 \leq i \leq n}(u_i)$
- Γ_{out}, read(u), highin(u), lowout(u), lowin(u)

Non-interférence

[Goguen&Meseguer 1982]

- purge : S × traces → S

$$purge(u, \langle \rangle) = \langle \rangle$$

$$purge(u, hist \cdot command(u')) = \begin{cases} purge(u, hist) \cdot command(u') & si\ h(u) \geqslant h(u') \\ purge(u, hist) & si\ h(u) < h(u') \end{cases}$$

- propriété

$$\forall u \in S, \forall w \in traces, \forall c \in \Gamma_{out}$$

$$out(u, w \cdot c(u)) = out(u, purge(u, w) \cdot c(u))$$

- assez proche de l'intuition mais aussi très forte

Non-interférence & co.

- Proche de l'intuition (vs. BLP)
  - interdit les canaux cachés
  - autorise des opérations (sans interférence)
- Limitations
  - interdit l'utilisation de canaux cryptographiques (même parfaits)
  - applicable seulement aux systèmes déterministes
- ***Non-déductibilité*** [Sutherland 1986] puis ***Non-interférence généralisée*** [McCullough 1987] visent les systèmes non-déterministes
- La ***restriction*** [McCullough 1990] vise à préserver la propriété en cas de composition de deux systèmes

Politiques de contrôle de flux

[Bieber&Cuppens 1992, d'Ausbourg 1994]

- *(o,t)* : entrées, sorties ou points internes (et temps)
- dépendance causale : $(o',t') \rightarrow (o,t)$ avec $t' < t$
- cône de causalité: $cone(o,t) = \{ (o',t') / (o',t') \rightarrow^* (o,t) \}$
- cône de dépendance: $dep(o,t) = \{ (o',t') / (o,t) \rightarrow^* (o',t') \}$
  - si *s* connait une sortie x_o il peut inférer $cone(x_o)$
  - si *s* connait une entrée x_i il peut inférer $dep(x_i)$

- confidentialité
- intégrité

$$\bigcup_{x_o \in O_s} cone(x_o) = Obs_s \subseteq R_s$$

$$\bigcup_{x_i \in A_s} cone(x_i) = Alt_s \subseteq W_s$$

Politiques spécifiques

- Politique d'intégrité de Clark et Wilson
  - données contraintes (CDI) et non-contraintes (UDI)
  - validation des procédures de traitement (TP) + procédure(s) de vérification d'intégrité (IVP)
  - gestion des relation entre données et procédures
- Muraille de Chine (ou Brewer-Nash)
  - étude de classes de conflits d'intérêts
  - dans un contexte dynamiques
- ...
  - données médicales
  - recommandations
  - **rôles**

Politique de sécurité

- Objectifs de sécurité : exemples
  - confidentialité : le dossier médical ne peut être consulté que par le patient ou son médecin traitant
  - intégrité : un chèque de plus de 1000 doit être validé par un ordonnateur et un comptable
  - disponibilité : si la carte et le PIN sont valides, le distributeur de billet doit fournir l'argent dans les 30 secondes
- Règles de sécurité : exemples
  - un fichier ne peut être lu que par les utilisateurs autorisés par le propriétaire du fichier
  - un message de type « chèque de + de 1000€ » n'est valide que s'il est signé par P1 et T2 et que les signatures sont valides
  - l'insertion d'une carte lance automatiquement l'action

Cohérence d'une politique

- La politique est cohérente si, partant d'un état quelconque où les objectifs sont satisfaits, il n'est pas possible d'atteindre, en respectant les règles, un état où ils ne sont plus satisfaits
- Intérêts d'un modèle formel
  - Décrire de manière précise les objectifs et les règles
  - Prouver des propriétés sur la politique (cohérence, complétude, ...) et sur son implémentation par le système informatique

Logique déontique
(une logique modale)
P, **O**, **F**
$(\Box, \Diamond)$

Politique, protection et contrôle d'accès

- Les règles doivent être mises en oeuvre par des mécanismes (matériels, logiciels)
- Facile à imaginer pour les règles du type « il est permis de... » ou « il est interdit de... » – mécanismes de protection – instructions privilégiées, contrôle d'accès à la mémoire, contrôle à l'ouverture des fichiers, etc.

  ➞ autorisation
- Difficile pour les règles du type « il est obligatoire de... » ou « il est recommandé de... »

  ➞ actions automatiques, gestion de ressources

Plan (1/2)

- Généralités
  - Propriétés de sécurité
  - Attaques
- Mise en œuvre dans les organisations
  - Fonctionnement de la sécurité dans une entreprise
  - Suivi des alertes de sécurité
  - Définition d'un schéma directeur sécurité
- Mécanismes de protection généraux
  - Cryptographie
  - Politiques de sécurité formelles
  - **Critères d'évaluation normalisés**

Les « Critères »

- Historique
  - TCSEC – Trusted Computer System Evaluation Criteria – DoD 1985 (Livre orange) et TNI – Trusted Network Interpretation of the TCSEC (Livre rouge)
  - ITSEC – Information Technology Security Evaluation Criteria (EEC 1991)
  - JCSEC, CTCPEC
  - CC – Common Criteria (norme ISO depuis ~2000)

Le livre orange : niveaux

D	Protection minimale	
C1	Protection discrétionnai	sécurité discrétionnair
C2		audit
B1	Protection obligatoire	labels
B2		protection structurée
B3		domaines de sécurité
A	Protection vérifiée	vérification

Le livre orange : critères (1/2)

- Doctrine de sécurité
  - Contrôle d'accès discrétionnaire
  - Réutilisation d'objet
  - Labels
  - Contrôle d'accès obligatoire
- Responsabilité
  - Identification et authentification
  - Cheminement sûr
  - Audit
- Assurance opérationnelle
  - Architecture du système
  - Intégrité du système
  - Analyse des canaux cachés
  - Gestion d'une installation
  - Reprise sûre

Le livre orange : critères (2/2)

- Assurance du cycle de vie
  - Essai de la sécurité
  - Spécification et vérification
  - Gestion de la configuration
  - Distribution sûre
- Documentation
  - Guide l'utilisateur
  - Manuel d'installation sûre
  - Documentation des essais
  - Documentation sur le concept de sécurité

ITSEC - Critères

- Classe de fonctionnalité
- Assurance de conformité : E1 à E6
- Assurance d'efficacité
  - Construction
    - Pertinence de la fonctionnalité
    - Cohésion de la fonctionnalité
    - Résistance des mécanismes
    - Estimation de la vulnérabilité de construction
  - Exploitation
    - Facilité d'emploi
    - Estimation de la vulnérabilité en exploitation

Nice quote on criteria

- CC – ISO 15408
  - Common Criteria

« For the most part, the protection profiles define away nearly all of the interesting threats that most systems face today. » *in* Fedora and CAPP, lwn.net, 10 dec. 2008.

Plan (2/2)

- Protection utilisées dans la pratique
  - **Protection réseau et *firewall***
  - Systèmes d'authentification
  - Chiffrement de flux et VPN
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
  - Détection d'intrusion
  - Audit, tests d'intrusion
  - Administration, exploitation et suivi de la sécurité
  - Observation et surveillance
- Protection des applications usuelles

Protection réseau et Firewall

- Principes de fonctionnements
  - Firewall avec suivi d'état
  - Firewall *proxy*
- Equipements commerciaux
  - Solutions logicielles
  - Equipements intégrés (hardware & software)
  - Firewall « personnel »
- Solutions open-source
- Filtres réseaux
  - Switches « intelligents » (VLAN, L4)
  - Routeurs (ACLs, anti-spoofing, etc.)

Solutions commerciales

- Leaders
  - FireWall-1 (CheckPoint)
  - PIX (Cisco)
- Challengers
  - Netscreen
  - Cyberguard
  - ISA Server (Microsoft)
  - IOS FW (Cisco)
  - …
- Solutions SOHO
  - SonicWall
  - WatchGuard
- Français
  - Netasq
  - Netwall (Evidian/Bull)
  - M>Wall (Matranet)
  - Arkoon
- …

Solutions open-source

- Linux/IPTable (Netfilter)
- Linux/IPChains
- IPFilter (Linux/Solaris/…)
- OpenBSD pf
- FreeBSD ~~ipfw~~ pf

Relais (*proxy*)

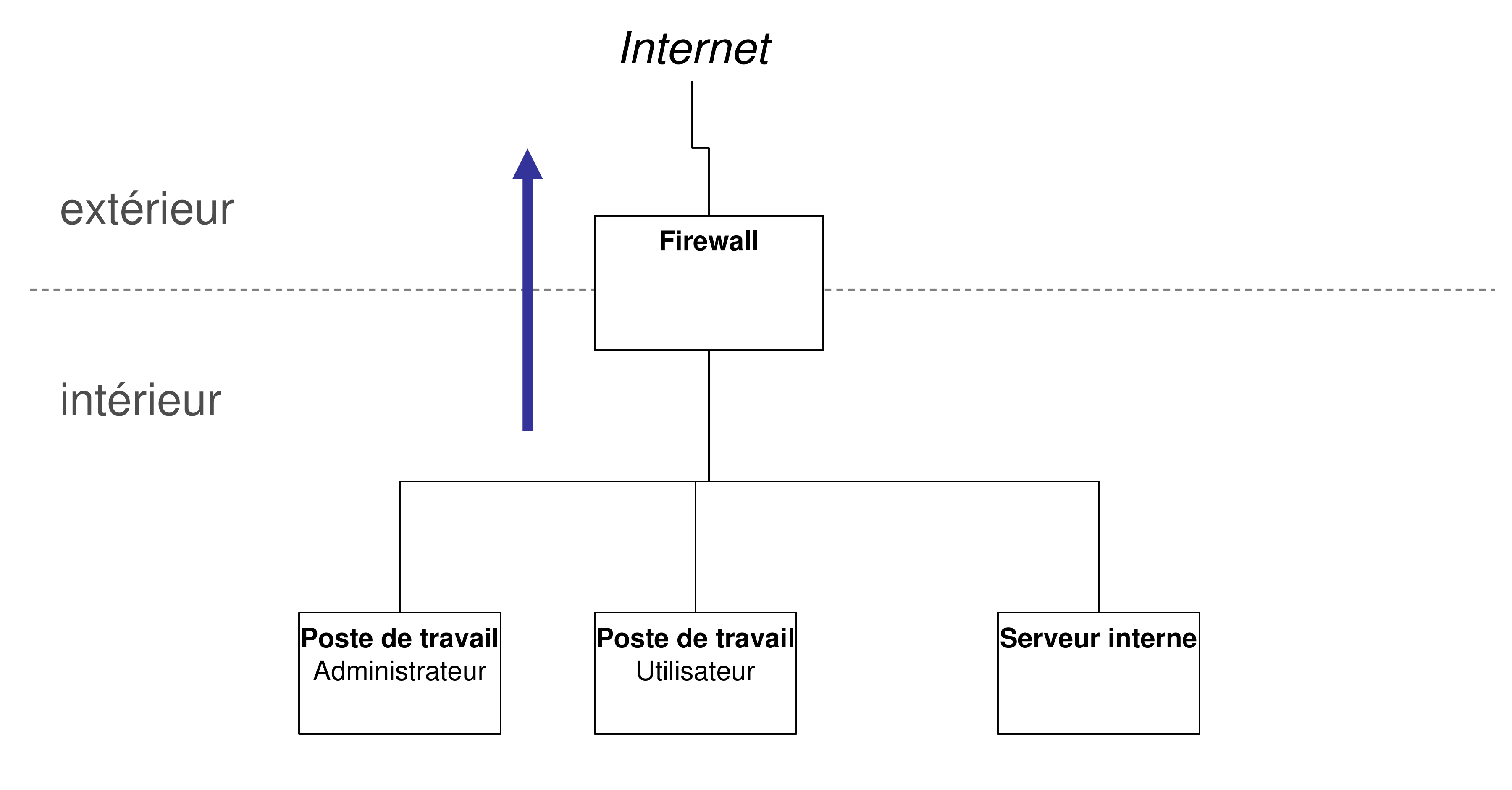
- Associé à des protocoles particuliers
  - HTTP
  - FTP
  - Telnet
  - X11
  - SOCKS
  - H.323 & co. ?
- Principaux intérêts
  - Prendre en charge des protocoles compliqués (comme FTP actif/passif)
  - Ajouter une autre authentification (si possible transparente)
  - Contrôler la validité protocolaire
  - Permettre un filtrage des commandes
- *Transparent proxying* : couplage noyau et *proxy*

Aspects architecturaux

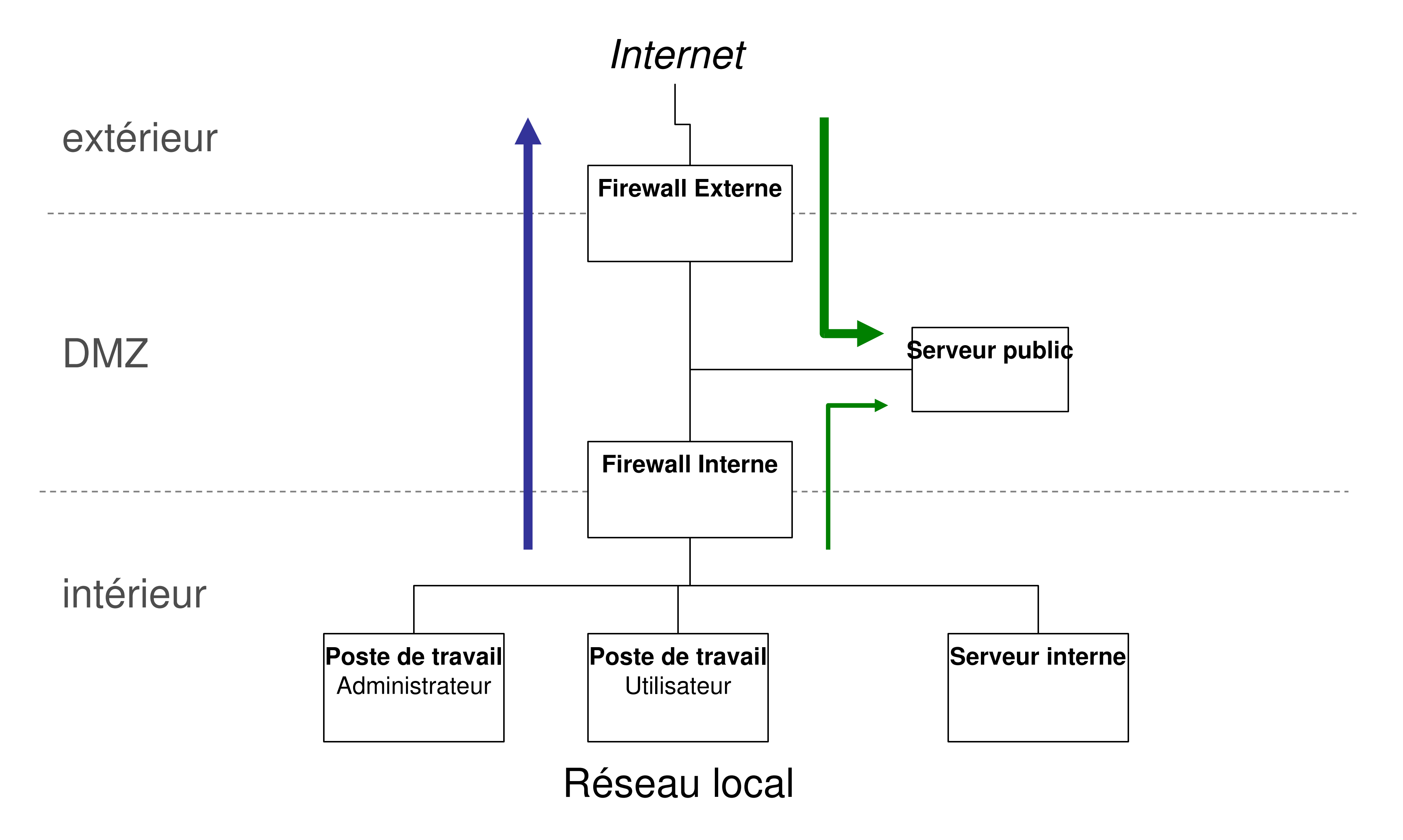
- Principes de fonctionnement
  - « niveaux » de sécurité et zones (DMZ)
  - Administration
  - Relais
  - Diversification
  - Environnement réels

Cheswick and S.M. Bellovin, *Firewalls and Internet security*, AddisonWesley, 1994

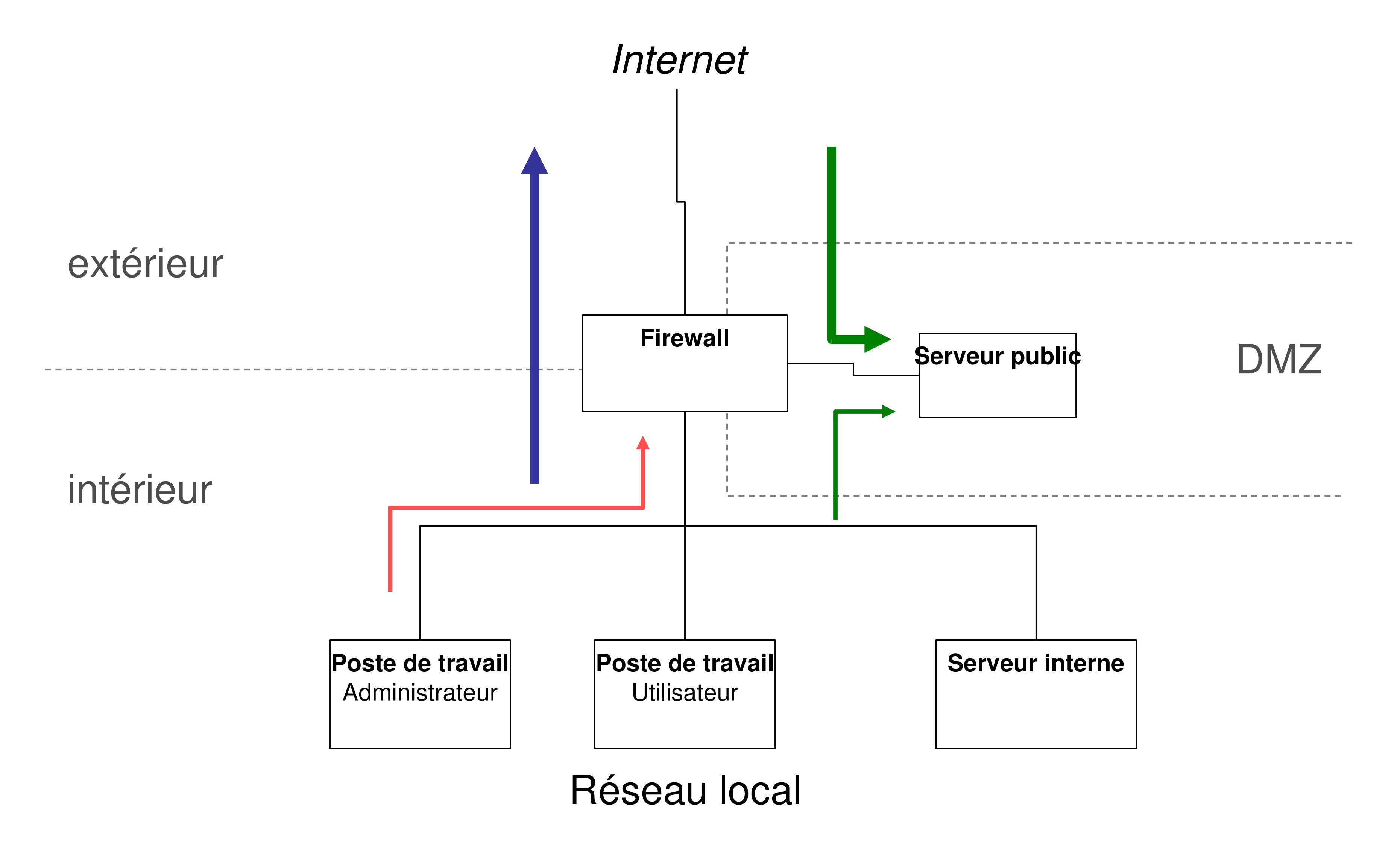
Diode


Internet
extérieur
intérieur
Firewall
Poste de travail
Administrateur
Poste de travail
Utilisateur
Serveur interne
Réseau local

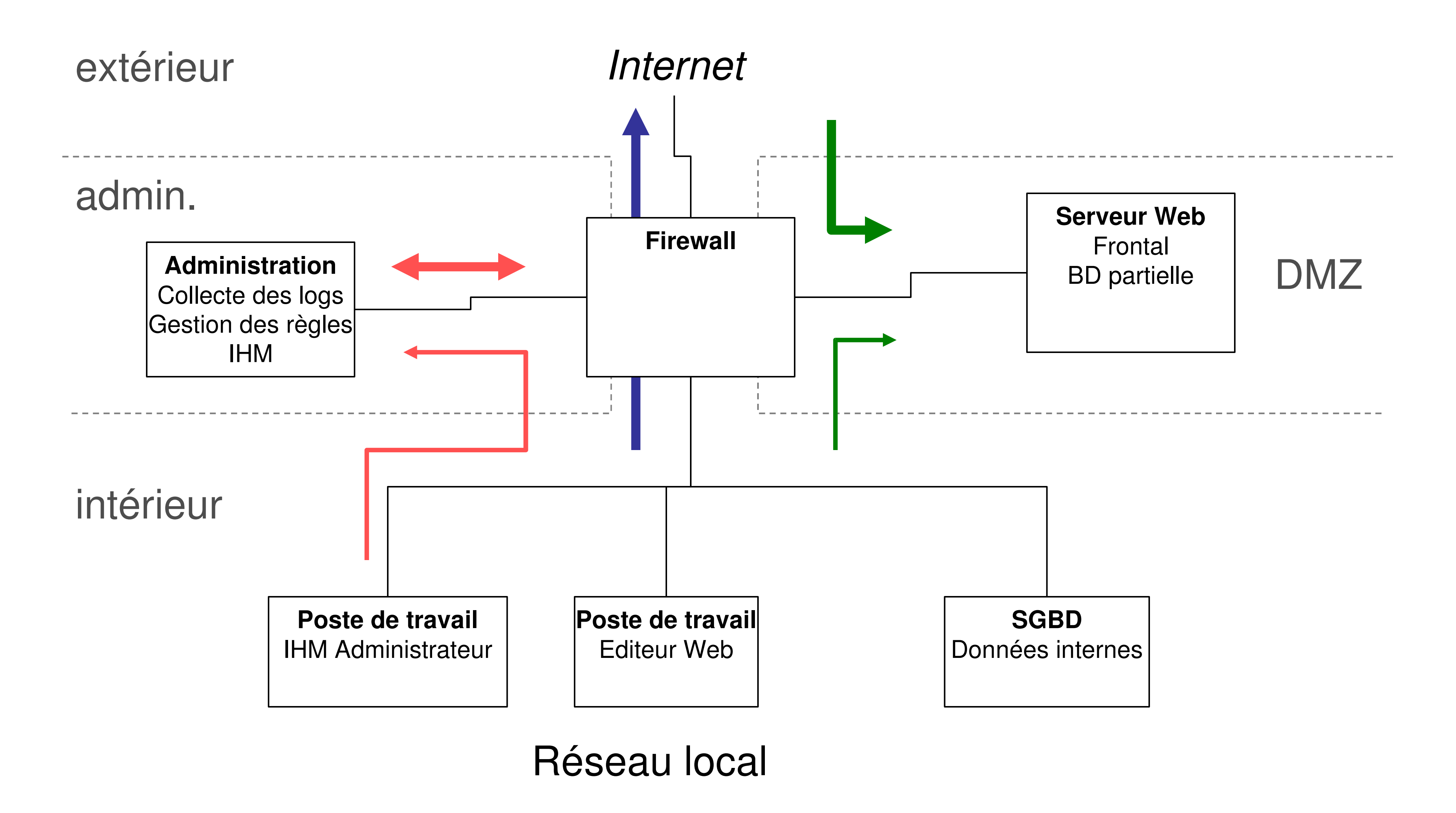
« DMZ » - Version historique



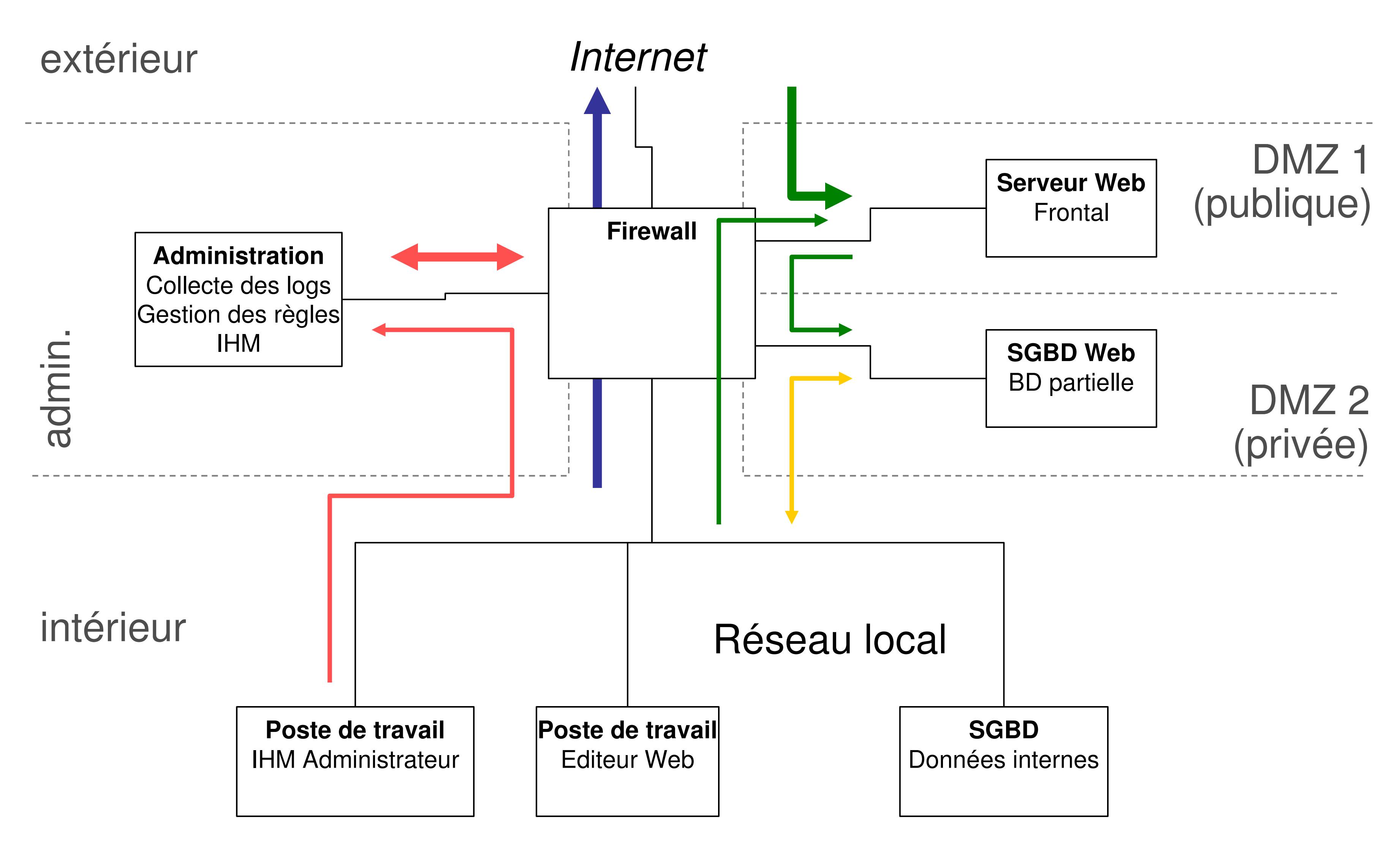
« DMZ » - Situation actuelle



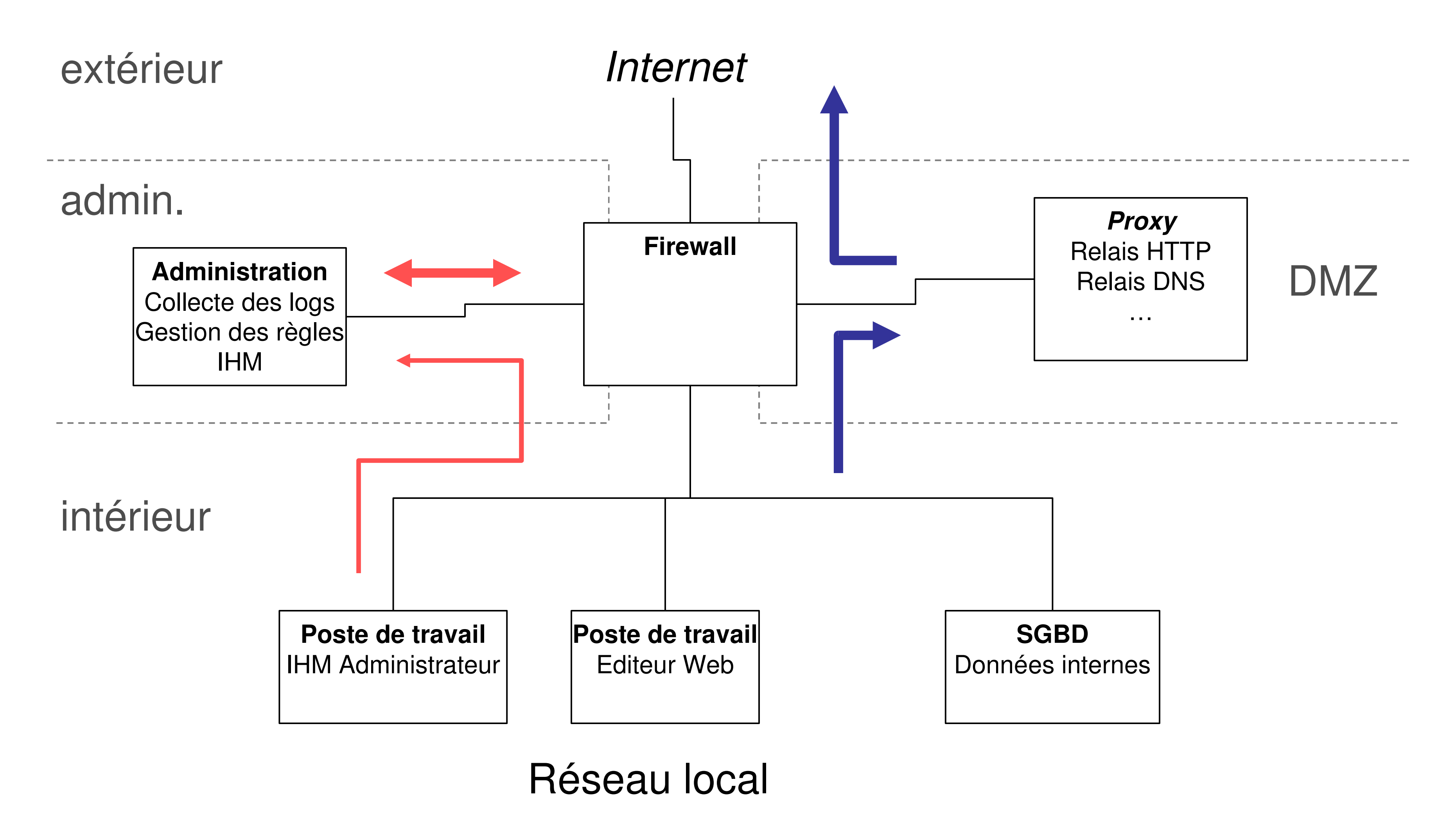
Administration



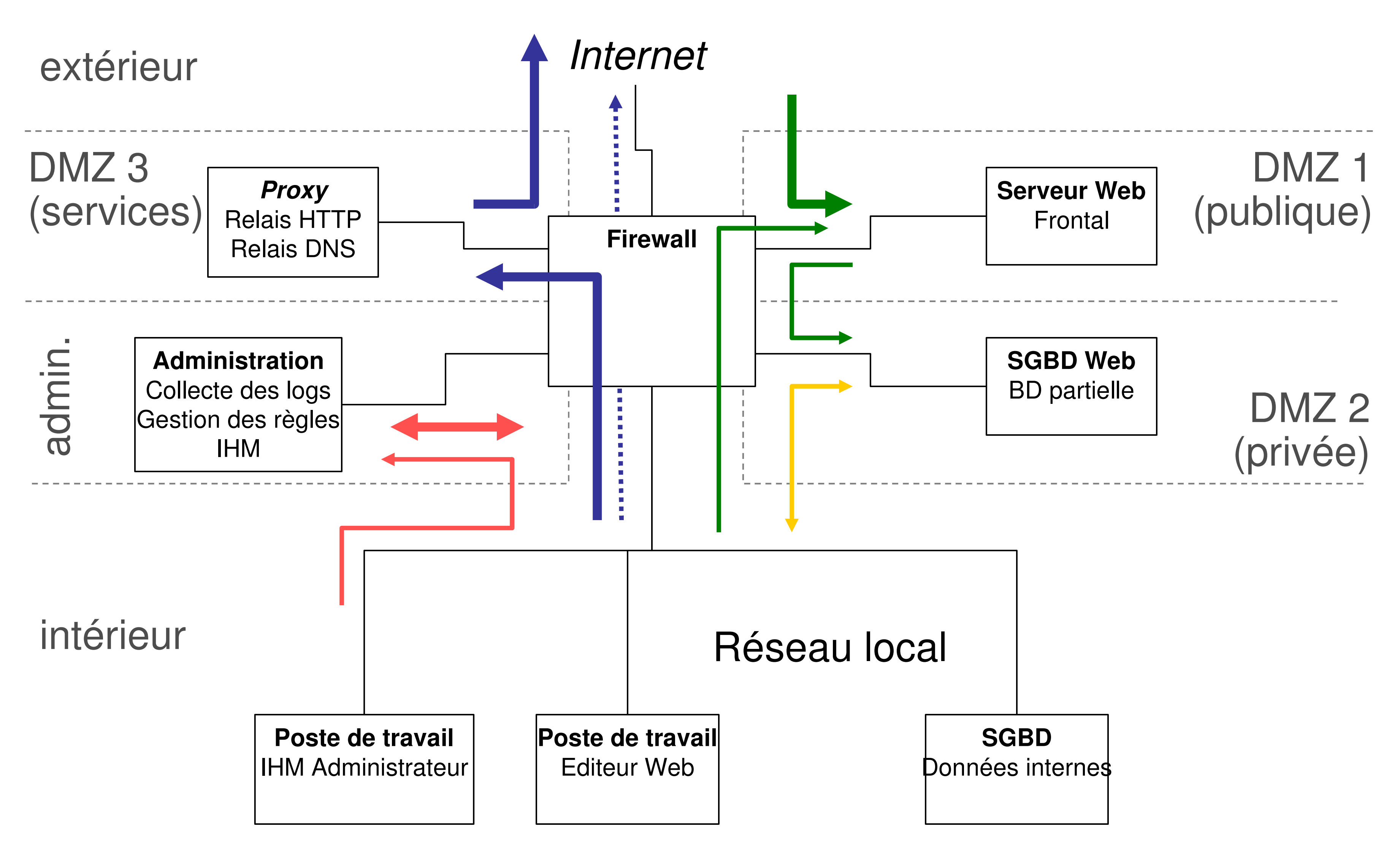
« 2 DMZ » – 5 interfaces



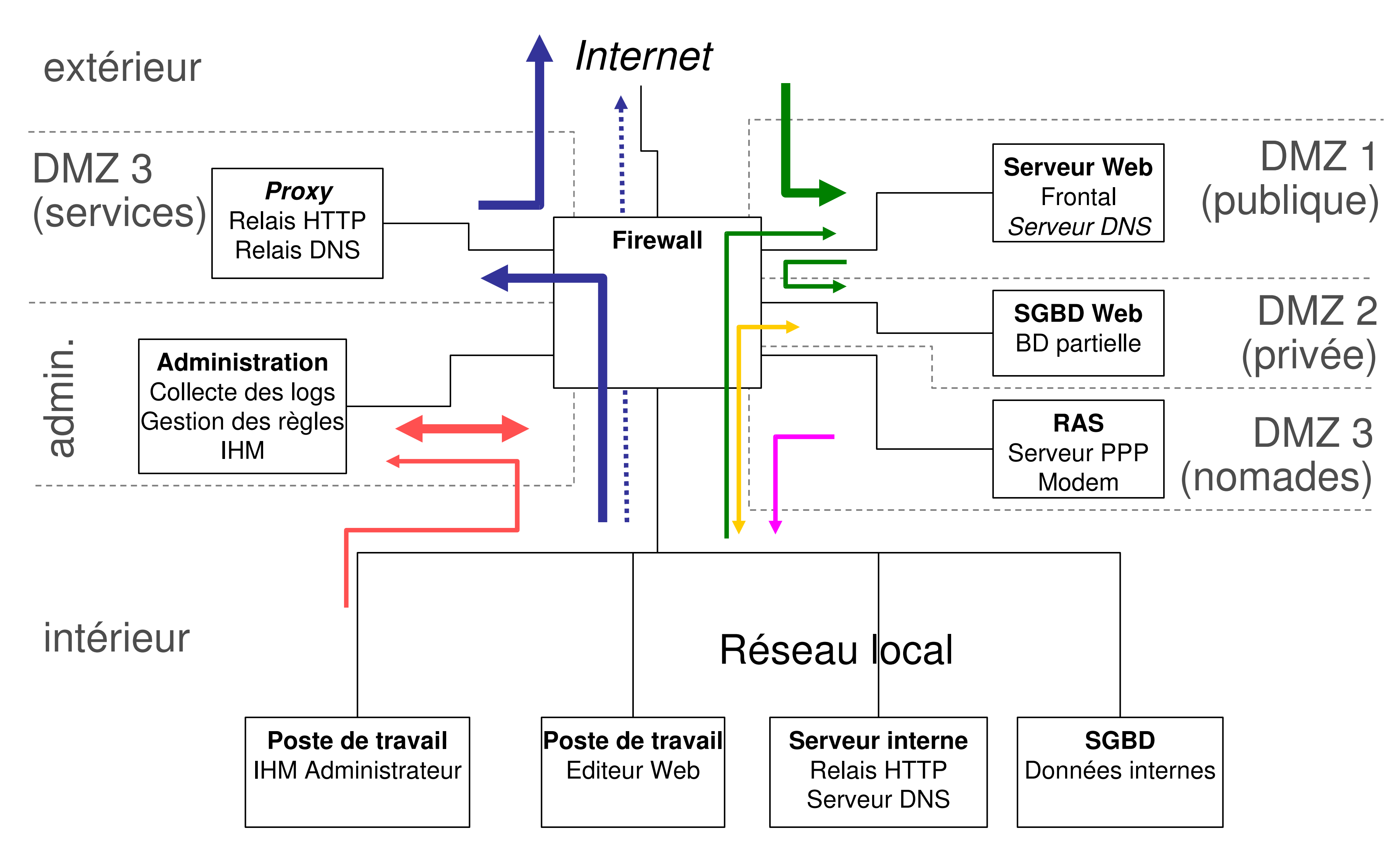
Autre usage d’une DMZ



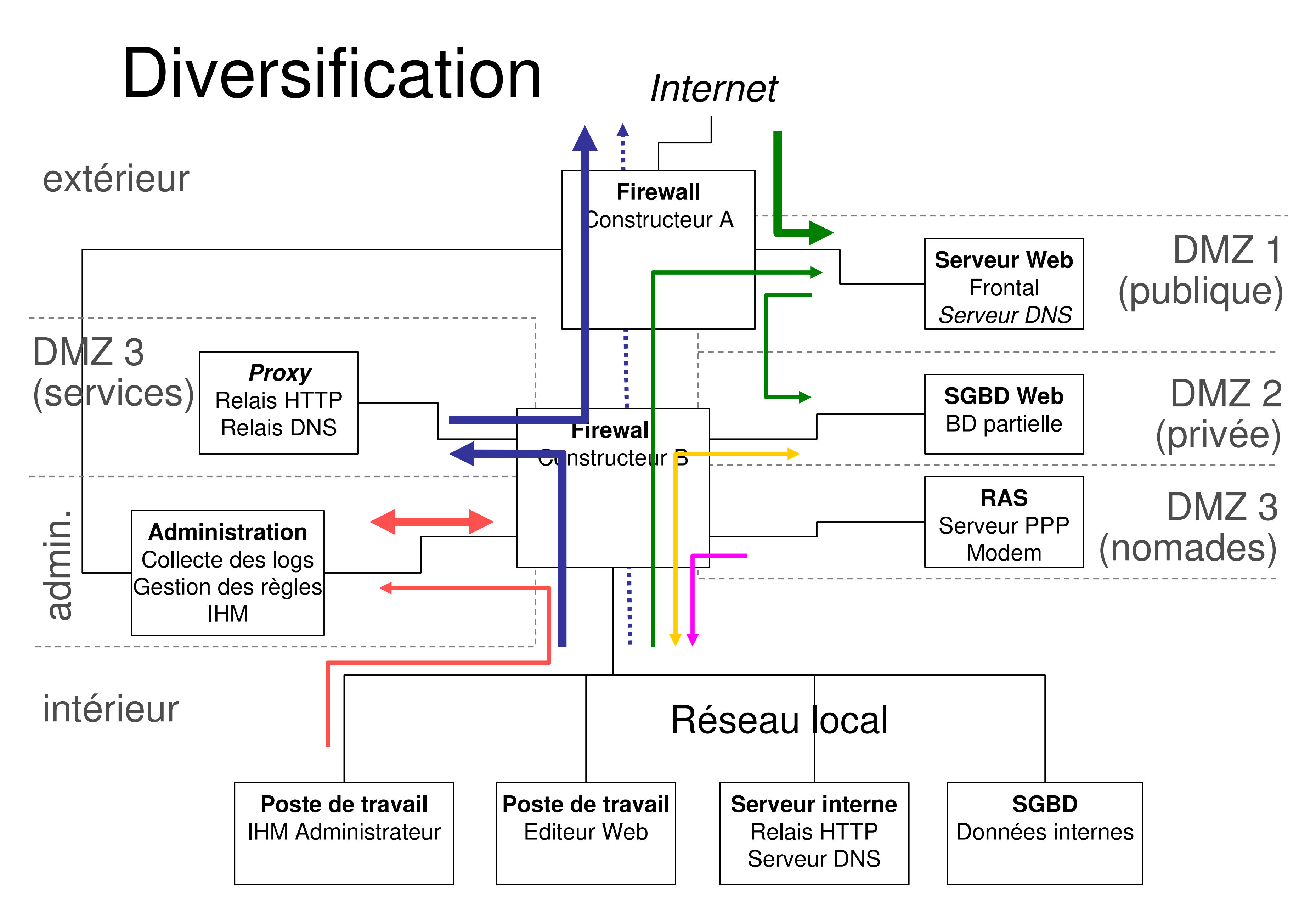
« 3 DMZ » – 6 interfaces



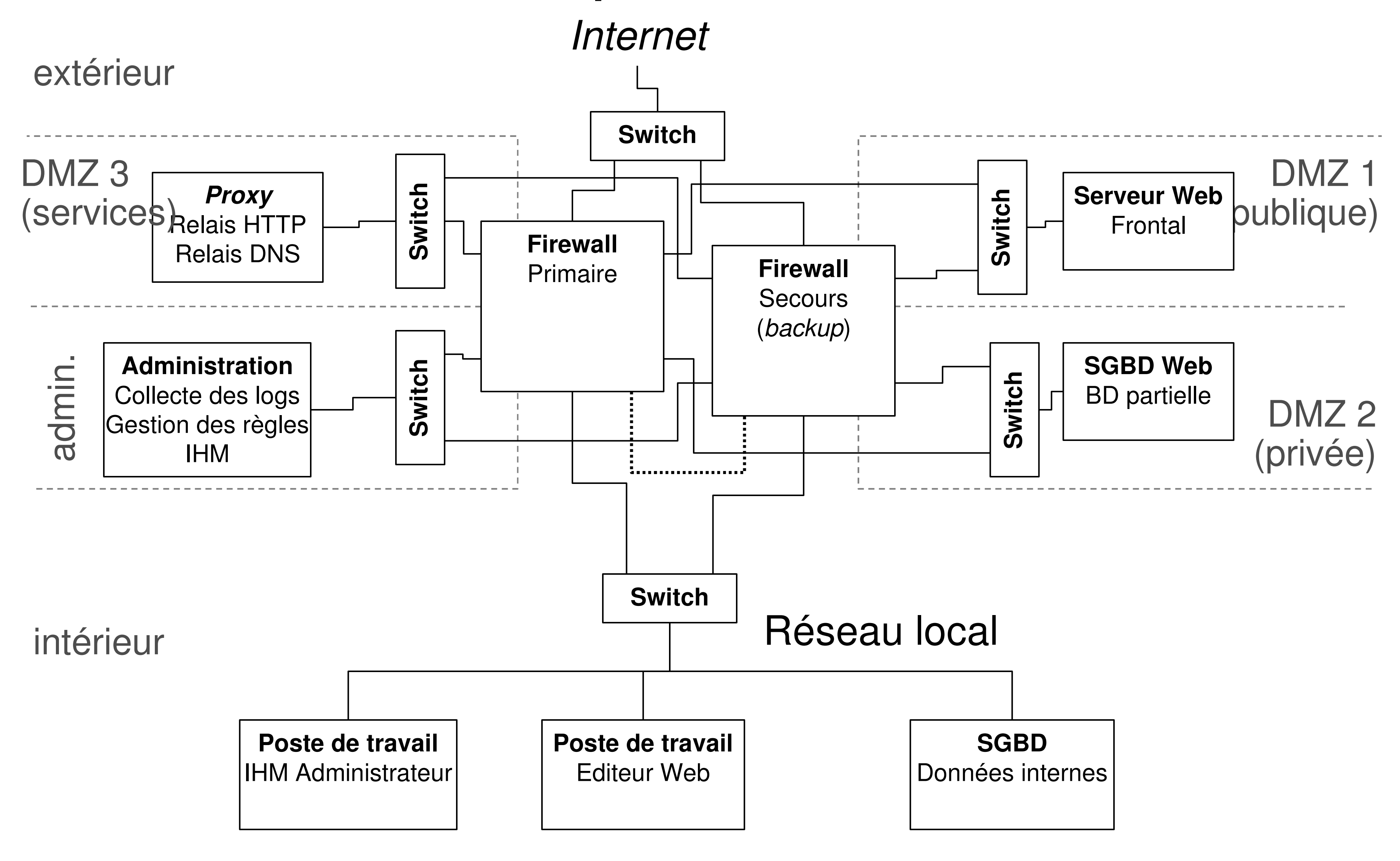
7 interfaces



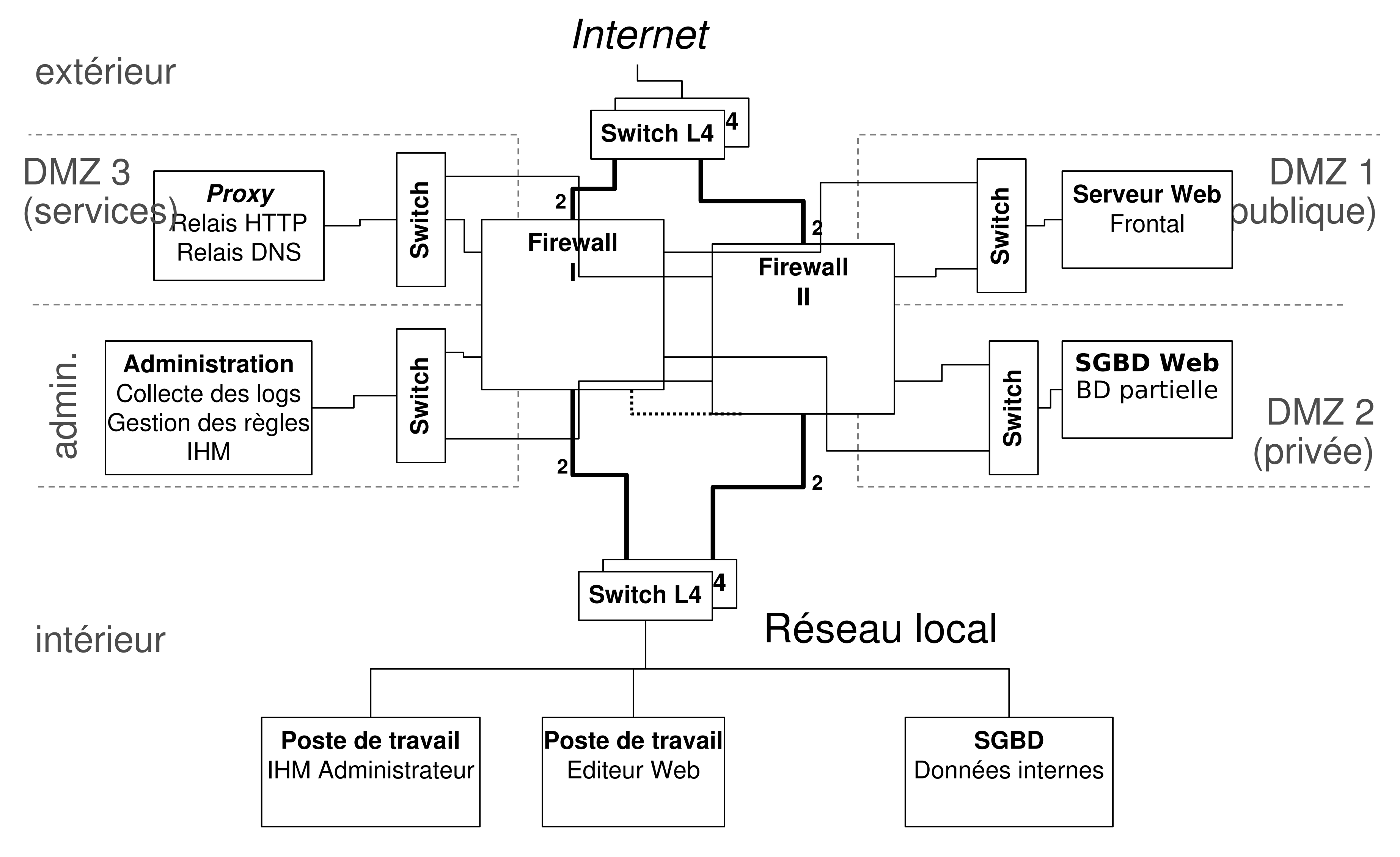
Diversification



Haute-disponibilité: *failover*



Haute-disponibilité : *load balancing*



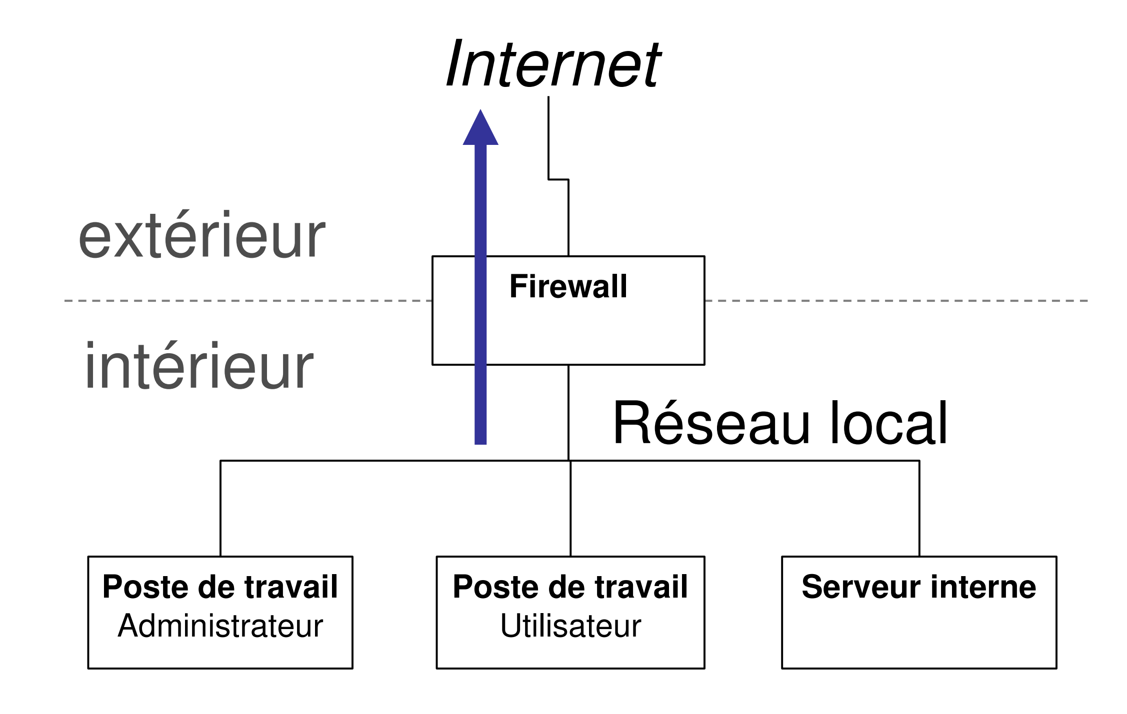
Diversification *et* haute-disponibilité avec équilibrage de charge pour un grand nombre de DMZ mises en oeuvre via des VLAN 802.1q

C’est possible.

Mais est-ce souhaitable ?

Translation d'adresses (NAT)

Multiplexage N @IP $\rightarrow$ P @IP (*NAT*)
Multiplexage N @(IP,TCP) $\rightarrow$ P@(IP,TCP) (*PAT*)
Association N @IP $\leftrightarrow$ N @IP (*static NAT*)



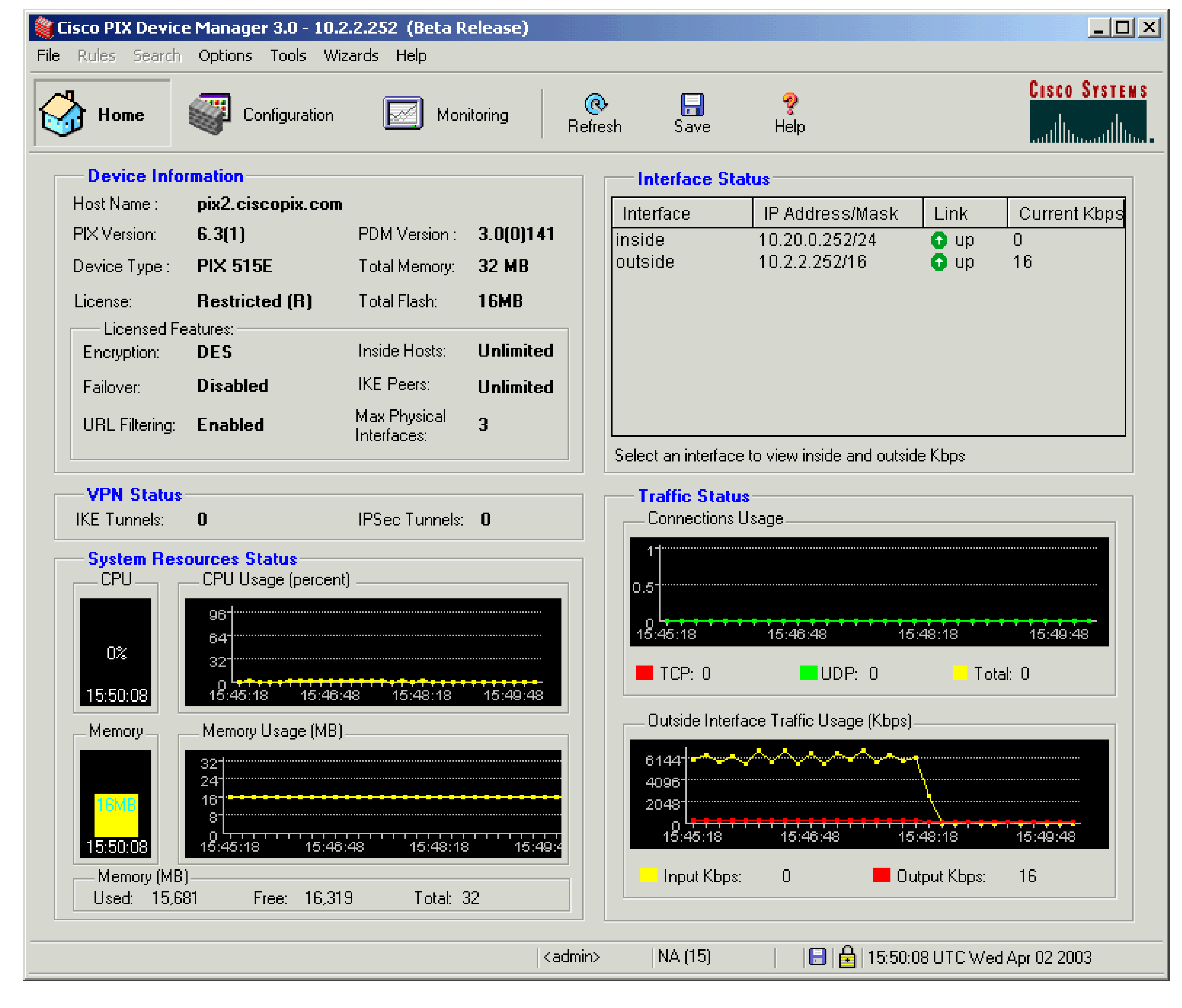
Translation d'adresses : compléments

- Le multiplexage est surtout naturel vis à vis du protocole orienté connexion (TCP) (à partir du port source)
- Il est également possible sur UDP, dans le cas des protocoles impliquant requête puis réponse (par ex.: DNS, etc.)
- Il peut aussi être introduit pour ICMP

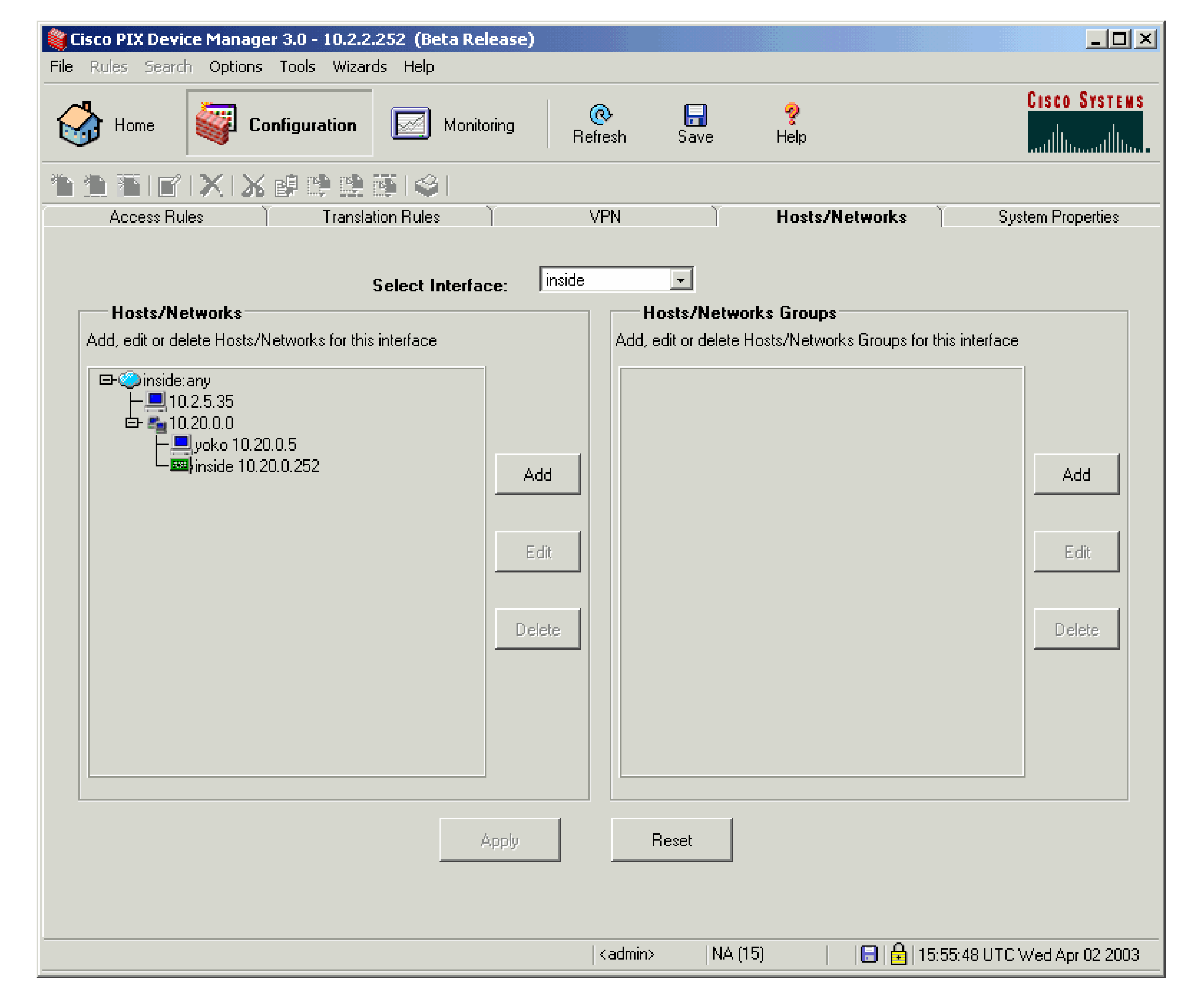
Firewall : fonctionnement interne

- Tables gérées
  - Tables d’état
  - Tables de translation
- Traces
- Fonctions de normalisation des paquets
- Analyses et fonctions avancées
  - Substitution des numéros de séquence
  - Inspection voire suivi protocolaire en mode noyau
  - Redirection vers des *proxy* en mode utilisateur

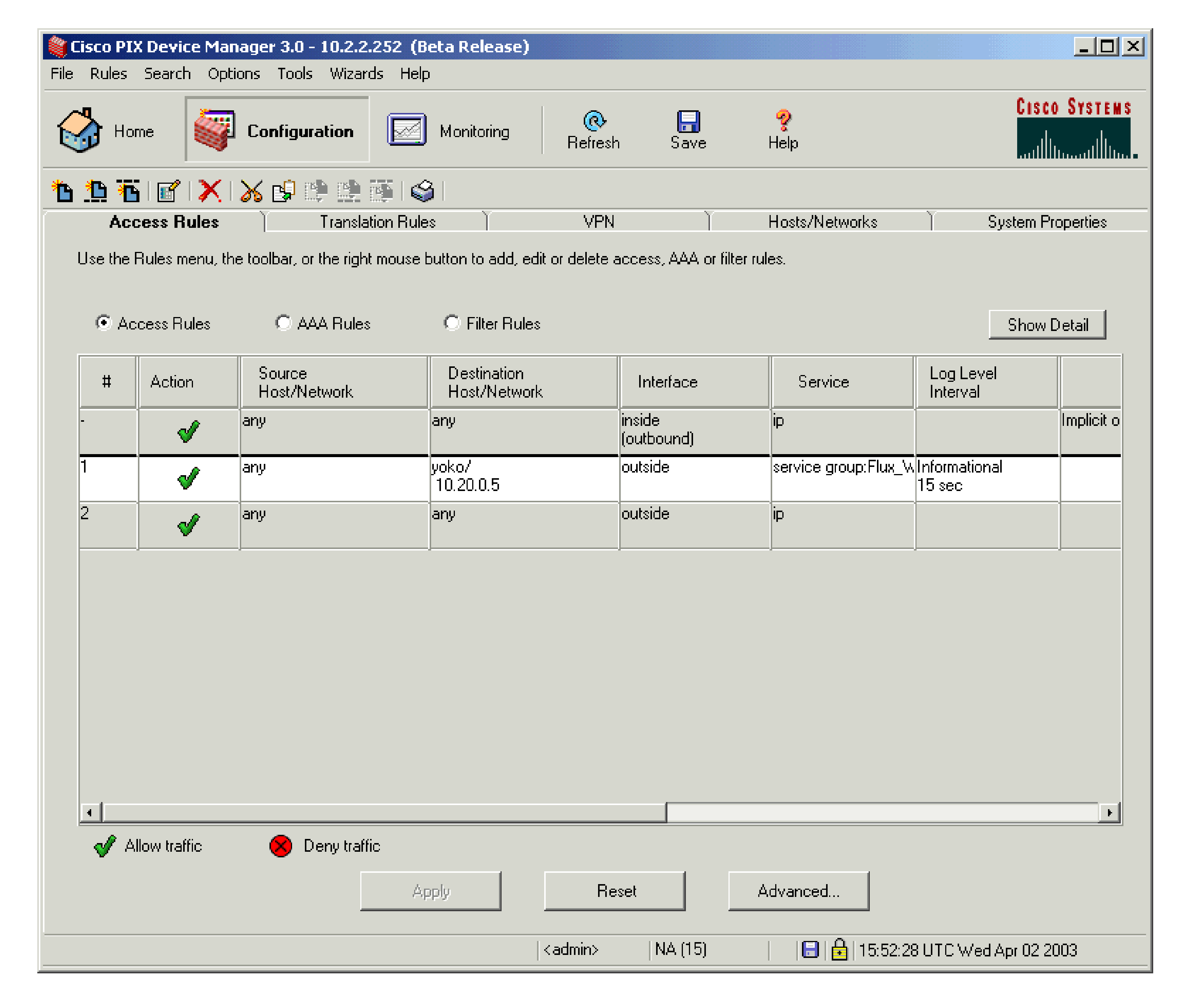
Exemple : Cisco PIX



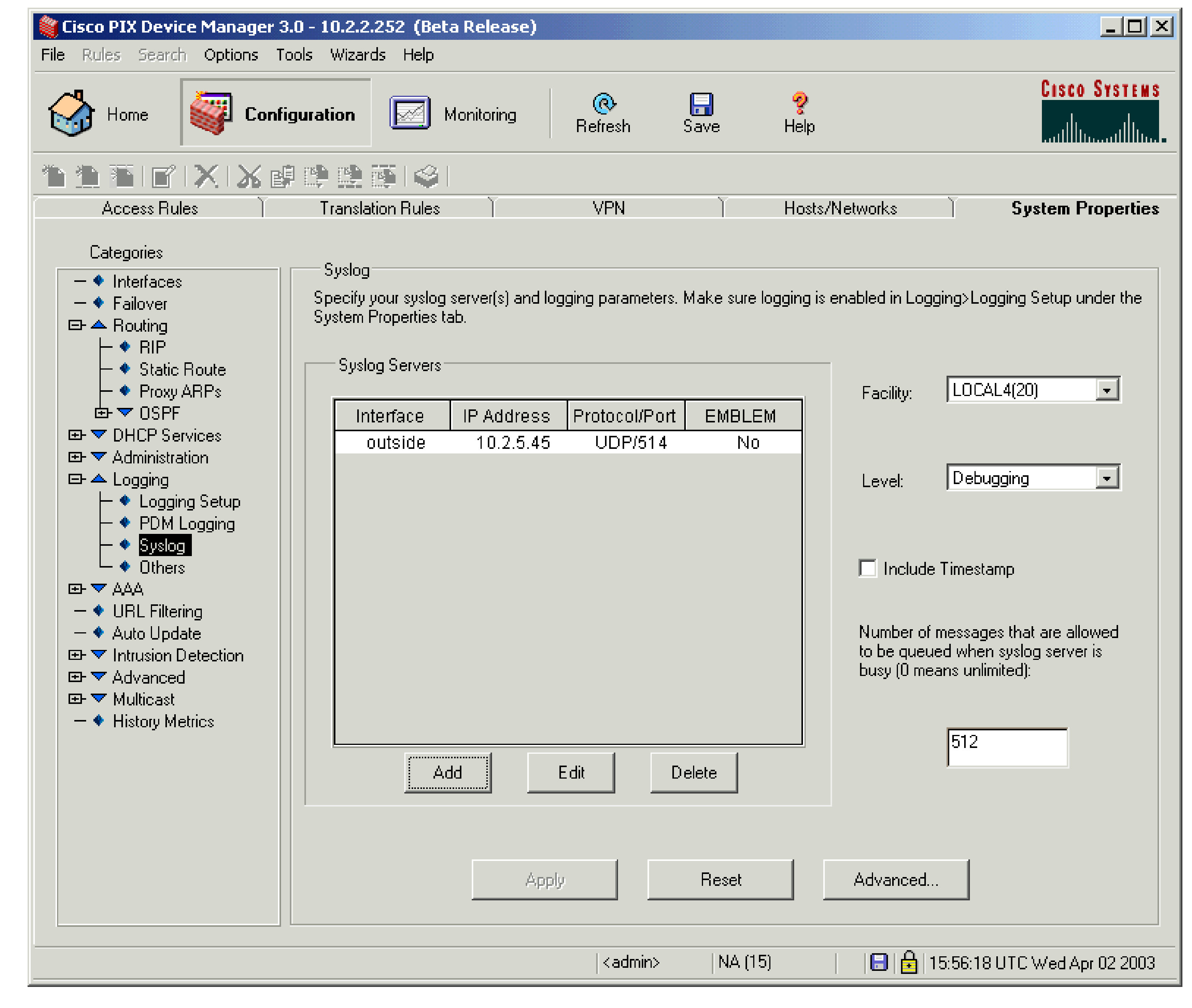
Exemple : Cisco PIX



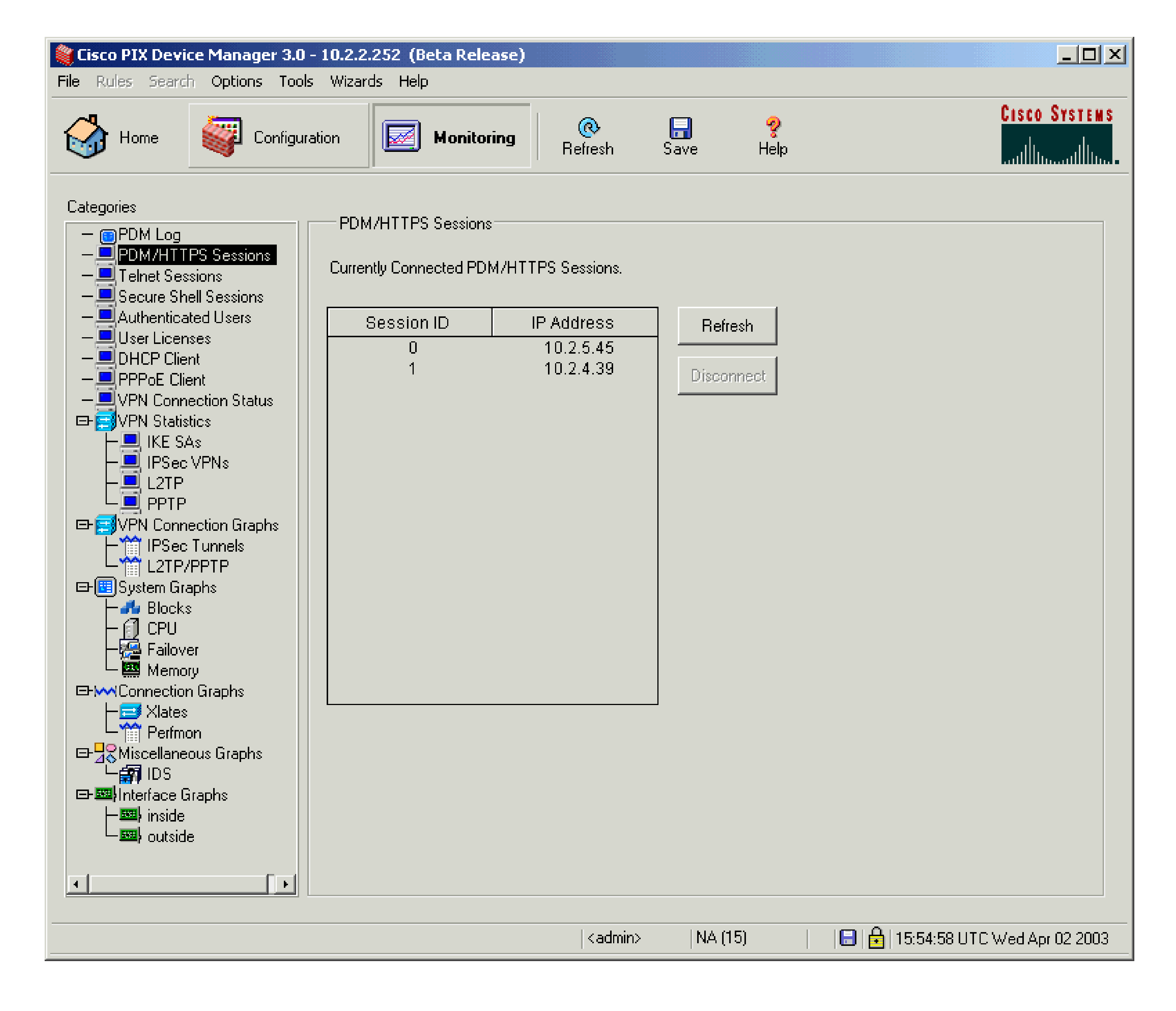
Exemple : Cisco PIX



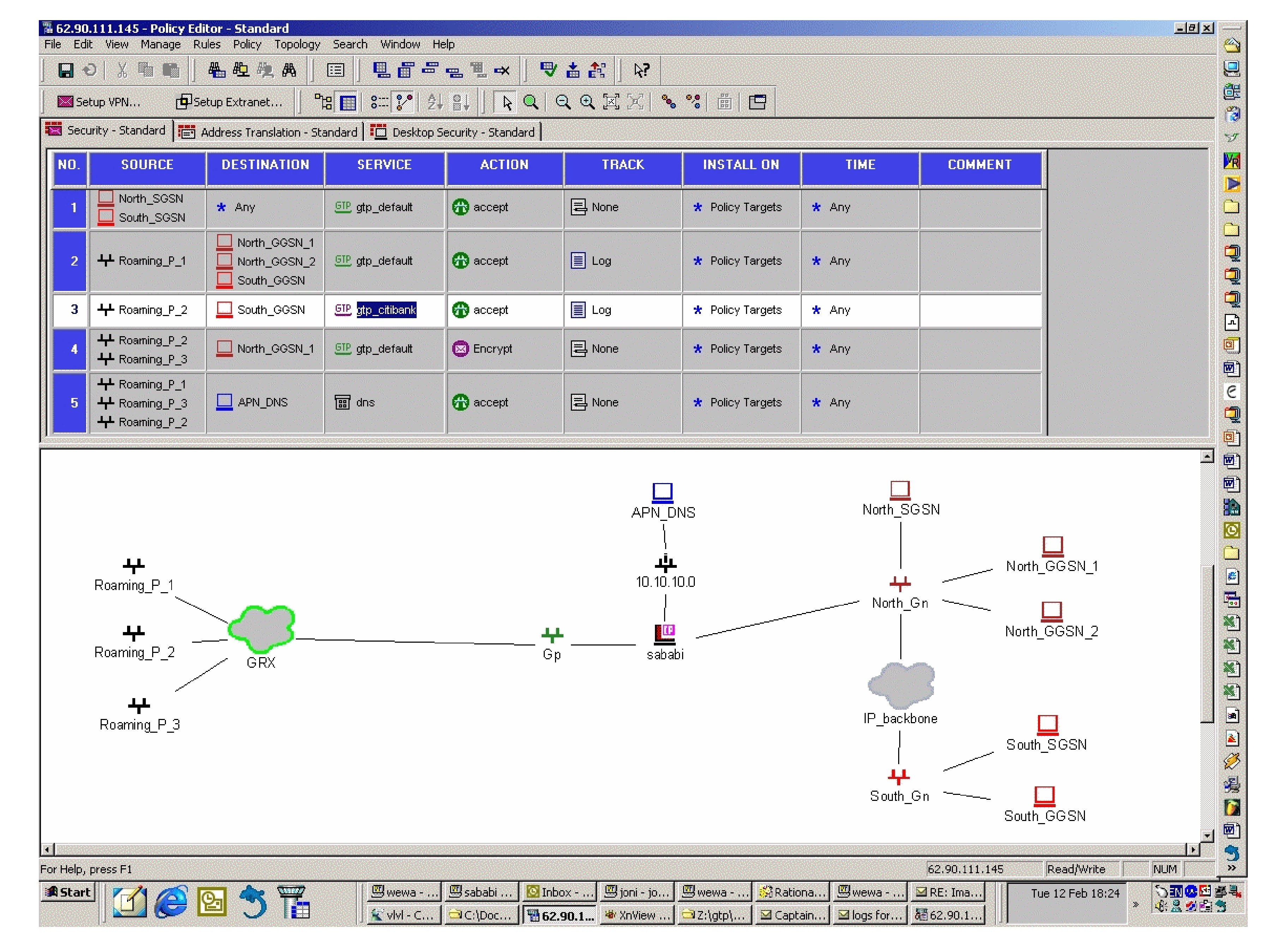
Exemple : Cisco PIX



Exemple : Cisco PIX

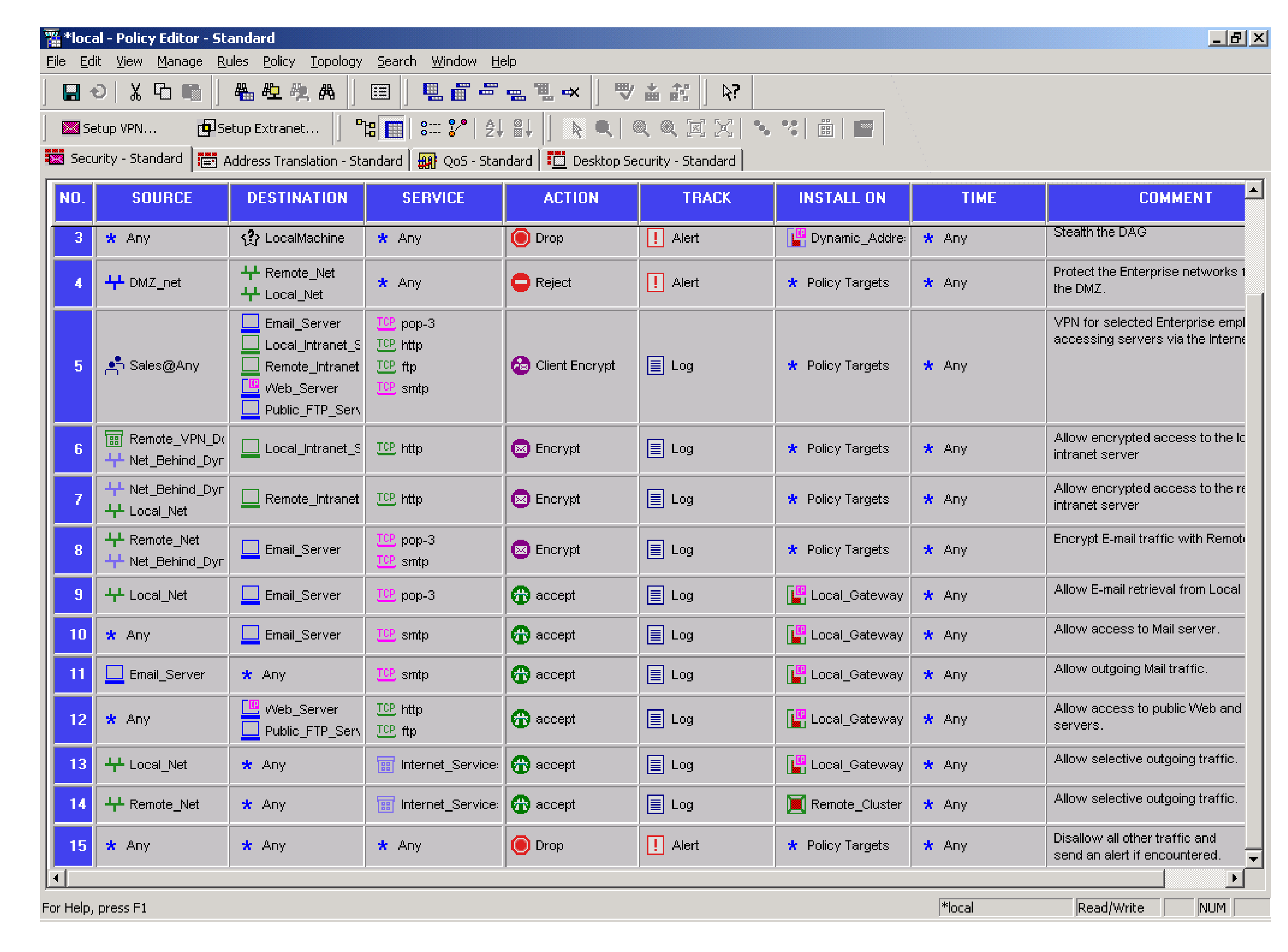


Ex. : CheckPoint Firewall-1



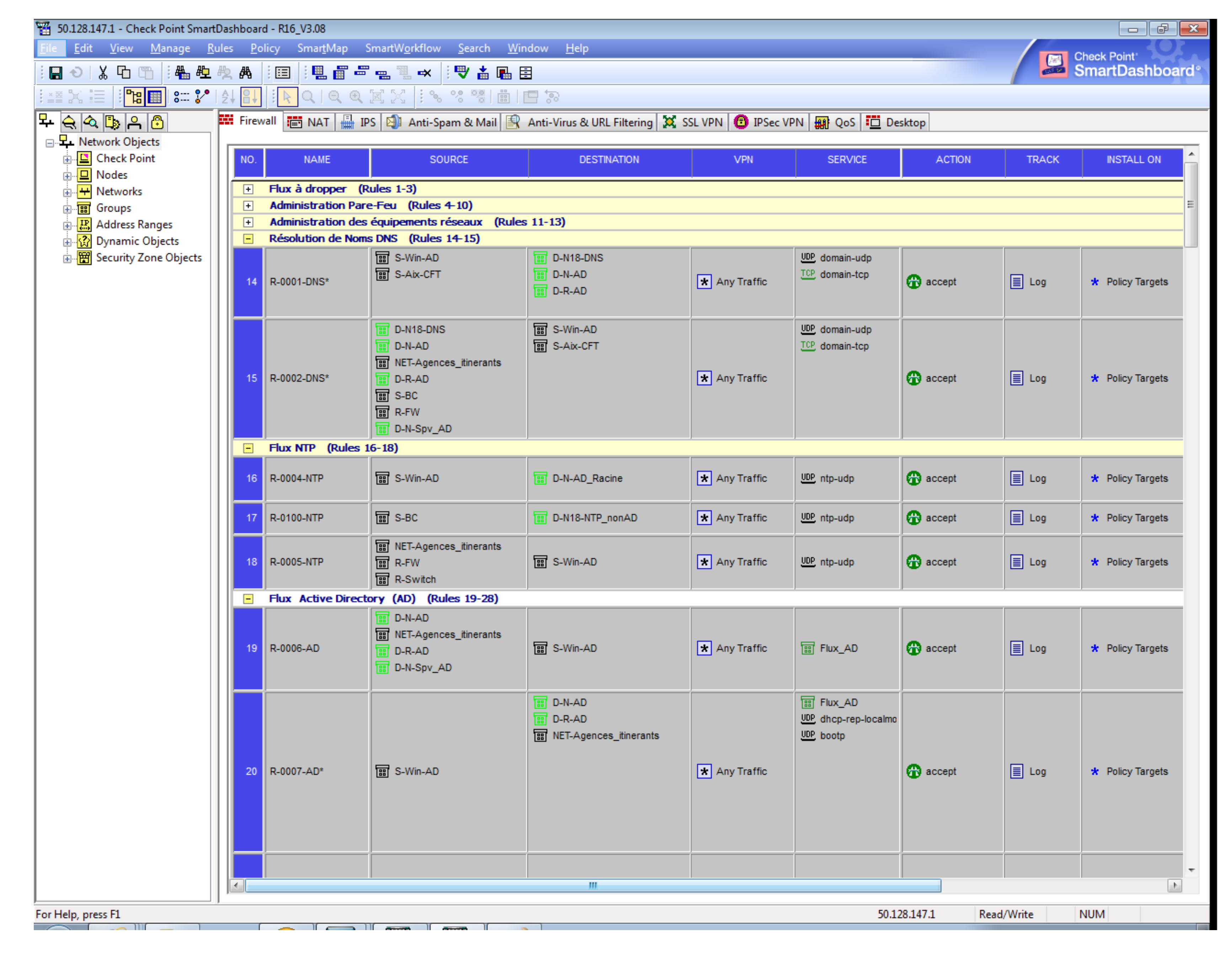
NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	North_SGSN South_SGSN	Any	gtp_default	accept	None	Policy Targets	Any	
2	Roaming_P_1	North_GGSN_1 North_GGSN_2 South_GGSN	gtp_default	accept	Log	Policy Targets	Any	
3	Roaming_P_2	South_GGSN	gtp_citibank	accept	Log	Policy Targets	Any	
4	Roaming_P_2 Roaming_P_3	North_GGSN_1	gtp_default	Encrypt	None	Policy Targets	Any	
5	Roaming_P_1 Roaming_P_3 Roaming_P_2	APN_DNS	dns	accept	None	Policy Targets	Any	

Ex. : CheckPoint Firewall-1

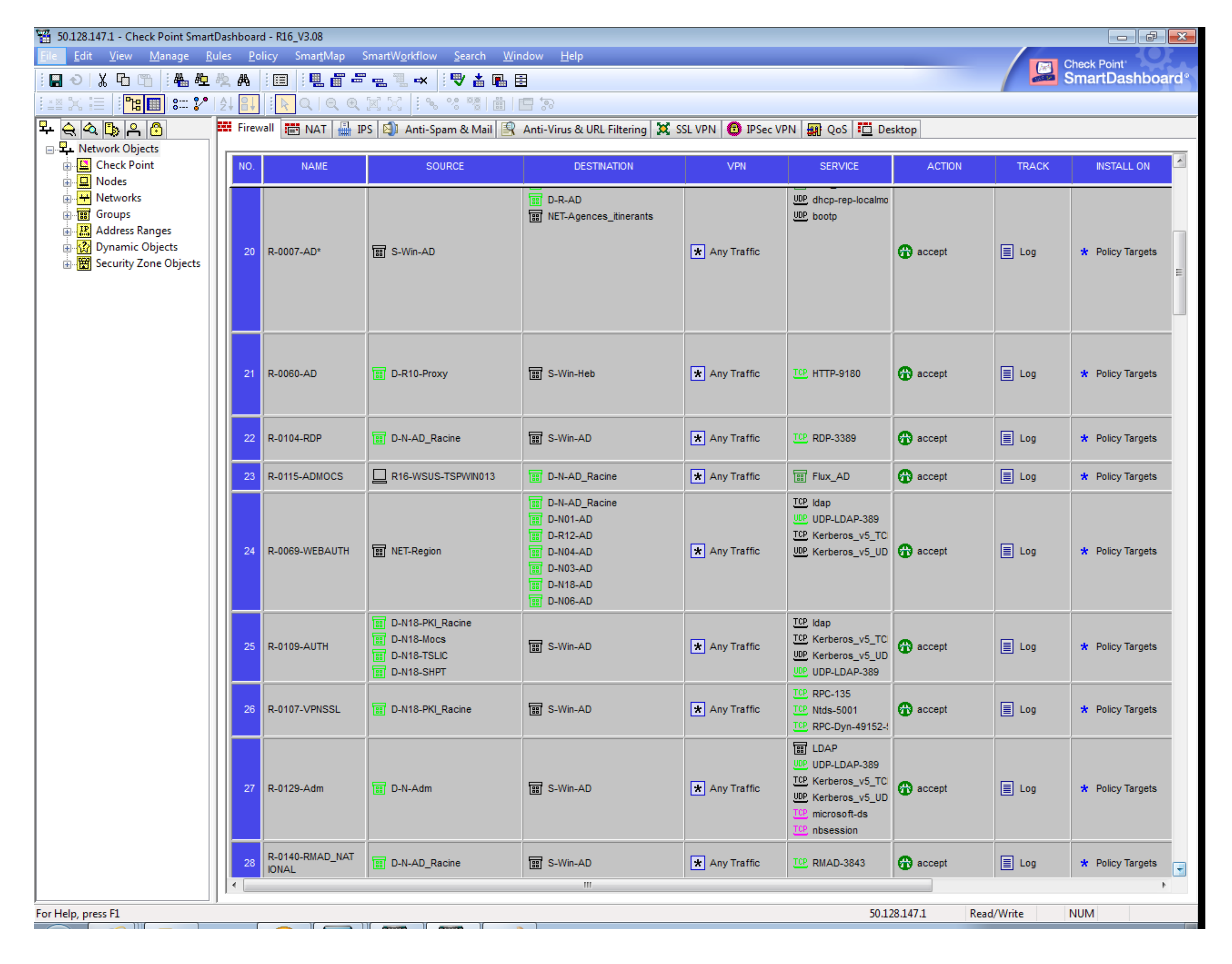


NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
3	Any	LocalMachine	Any	Drop	Alert	Dynamic_Addre:	Any	Stealth the DAG
4	DMZ_net	Remote_Net Local_Net	Any	Reject	Alert	Policy Targets	Any	Protect the Enterprise networks t the DMZ.
5	Sales@Any	Email_Server Local_Intranet_S Remote_Intranet Web_Server Public_FTP_Serv	pop-3 http ftp smtp	Client Encrypt	Log	Policy Targets	Any	VPN for selected Enterprise empl accessing servers via the Interne
6	Remote_VPN_D Net_Behind_Dyr	Local_Intranet_S	http	Encrypt	Log	Policy Targets	Any	Allow encrypted access to the lo intranet server
7	Net_Behind_Dyr Local_Net	Remote_Intranet	http	Encrypt	Log	Policy Targets	Any	Allow encrypted access to the re intranet server
8	Remote_Net Net_Behind_Dyr	Email_Server	pop-3 smtp	Encrypt	Log	Policy Targets	Any	Encrypt E-mail traffic with Remot
9	Local_Net	Email_Server	pop-3	accept	Log	Local_Gateway	Any	Allow E-mail retrieval from Local
10	Any	Email_Server	smtp	accept	Log	Local_Gateway	Any	Allow access to Mail server.
11	Email_Server	Any	smtp	accept	Log	Local_Gateway	Any	Allow outgoing Mail traffic.
12	Any	Web_Server Public_FTP_Serv	http ftp	accept	Log	Local_Gateway	Any	Allow access to public Web and servers.
13	Local_Net	Any	Internet_Service:	accept	Log	Local_Gateway	Any	Allow selective outgoing traffic.
14	Remote_Net	Any	Internet_Service:	accept	Log	Remote_Cluster	Any	Allow selective outgoing traffic.
15	Any	Any	Any	Drop	Alert	Policy Targets	Any	Disallow all other traffic and send an alert if encountered.

Ex. : CheckPoint Firewall-1

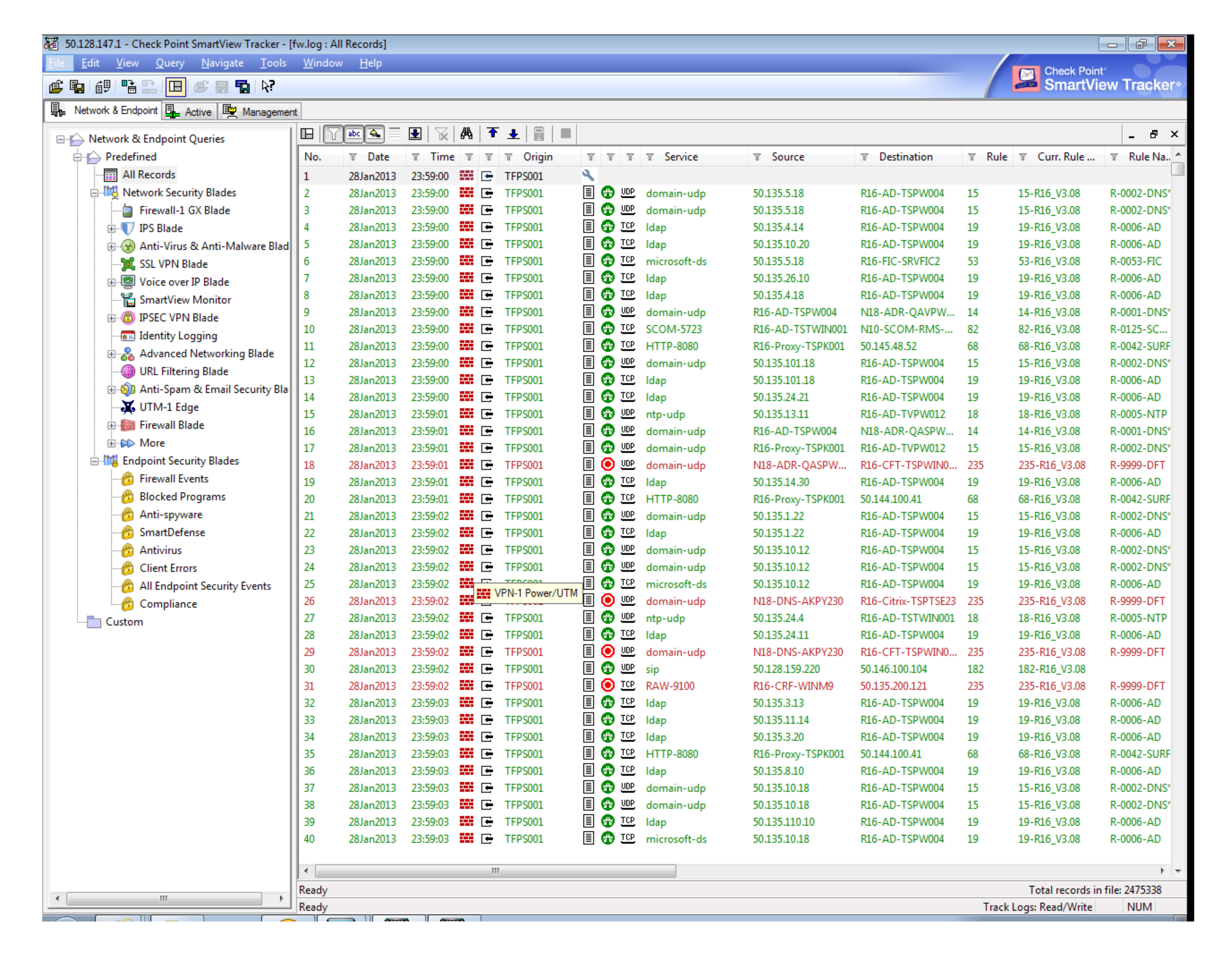


Ex. : CheckPoint Firewall-1

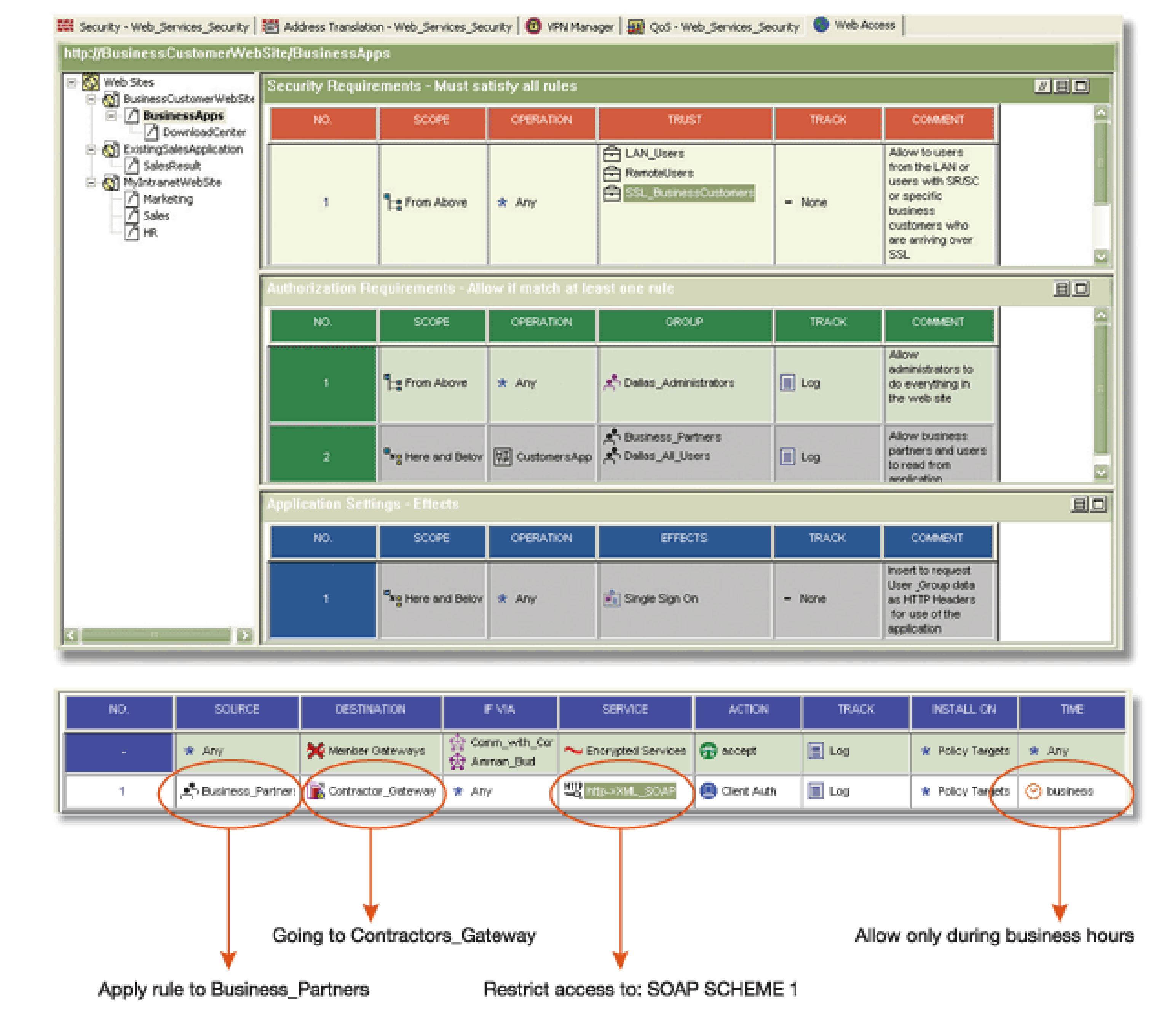


NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON
20	R-0007-AD*	S-Win-AD	D-R-AD NET-Agences_itinerants	Any Traffic	dhcp-rep-localmo bootp	accept	Log	Policy Targets
21	R-0060-AD	D-R10-Proxy	S-Win-Heb	Any Traffic	HTTP-9180	accept	Log	Policy Targets
22	R-0104-RDP	D-N-AD_Racine	S-Win-AD	Any Traffic	RDP-3389	accept	Log	Policy Targets
23	R-0115-ADMOCS	R16-WSUS-TSPWIN013	D-N-AD_Racine	Any Traffic	Flux_AD	accept	Log	Policy Targets
24	R-0069-WEBAUTH	NET-Region	D-N-AD_Racine D-N01-AD D-R12-AD D-N04-AD D-N03-AD D-N18-AD D-N06-AD	Any Traffic	ldap UDP-LDAP-389 Kerberos_v5_TC Kerberos_v5_UD	accept	Log	Policy Targets
25	R-0109-AUTH	D-N18-PKI_Racine D-N18-Mocs D-N18-TSLIC D-N18-SHPT	S-Win-AD	Any Traffic	ldap Kerberos_v5_TC Kerberos_v5_UD UDP-LDAP-389	accept	Log	Policy Targets
26	R-0107-VPNSSL	D-N18-PKI_Racine	S-Win-AD	Any Traffic	RPC-135 Ntds-5001 RPC-Dyn-49152-!	accept	Log	Policy Targets
27	R-0129-Adm	D-N-Adm	S-Win-AD	Any Traffic	LDAP UDP-LDAP-389 Kerberos_v5_TC Kerberos_v5_UD microsoft-ds nbsession	accept	Log	Policy Targets
28	R-0140-RMAD_NATIONAL	D-N-AD_Racine	S-Win-AD	Any Traffic	RMAD-3843	accept	Log	Policy Targets

Ex. : CheckPoint Firewall-1



Ex. : CheckPoint Firewall-1



Comment gérer une autorisation dans la pratique ?

- Une application
  - vlc (césaco?)
  - http://mafreebox.freebox.fr/freeboxtv/playlist.m3u (on comprend mieux)
- Ne « marche pas », « Un numéro de porte ? »
- Premier pas

```
ortalo@hurricane:~$ ping -c 1 mafreebox.freebox.fr
PING freeplayer.freebox.fr (212.27.38.253) 56(84) bytes of data.
64 bytes from freeplayer.freebox.fr (212.27.38.253): icmp_seq=1 ttl=64
   time=1.16 ms
--- freeplayer.freebox.fr ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.168/1.168/1.168/0.000 ms
ortalo@hurricane:~$ tethereal -i eth1 host 212.27.38.253
```

...rien...

- Déterminer (toutes) les sources et destinations impliquées
  - IP_{eth1} et `212.27.38.253` (hmm...)
- Approche expérimentale : repérer les échecs les uns après les autres tout en contrôlant le trafic réseau

DROPPED IN= OUT=eth1 **SRC=81.56.84.23 DST=212.27.38.253** LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48783 DF PROTO=TCP SPT=1047 **DPT=80** SEQ=1610765695 ACK=0 WINDOW=5840 RES=0x00 SYN URGP=0 OPT (020405B40101040201030300)

DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48784 DF PROTO=TCP SPT=1047 **DPT=80** SEQ=1610765695 ACK=0 WINDOW=5840 RES=0x00 SYN URGP=0 OPT (020405B40101040201030300)

DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=1506 DF PROTO=TCP SPT=1048 **DPT=80** SEQ=1611201085 ACK=0 WINDOW=5840 RES=0x00 SYN URGP=0 OPT (020405B40101040201030300)

- On ré-autorise HTTP

```
DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=52 TOS=0x00
   PREC=0x00 TTL=64 ID=22928 DF PROTO=TCP SPT=1082 DPT=554 SEQ=2534727009
   ACK=0 WINDOW=5840 RES=0x00 SYN URGP=0 OPT (020405B40101040201030300)
DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=52 TOS=0x00
   PREC=0x00 TTL=64 ID=22929 DF PROTO=TCP SPT=1082 DPT=554 SEQ=2534727009
   ACK=0 WINDOW=5840 RES=0x00 SYN URGP=0 OPT (020405B40101040201030300)
```

- On autorise TCP/554 sortant (?)

```
DROPPED IN=eth1 OUT= MAC=00:50:bf:29:e7:88:00:07:cb:05:ec:fc:08:00
   SRC=212.27.38.253 DST=81.56.84.23 LEN=1356 TOS=0x00 PREC=0xE0 TTL=57
   ID=18727 DF PROTO=UDP SPT=32803 DPT=1044 LEN=1336
DROPPED IN=eth1 OUT= MAC=00:50:bf:29:e7:88:00:07:cb:05:ec:fc:08:00
   SRC=212.27.38.253 DST=81.56.84.23 LEN=1356 TOS=0x00 PREC=0xE0 TTL=57
   ID=18982 DF PROTO=UDP SPT=32803 DPT=1044 LEN=1336
```

- La liste de diffusion arrive
- On autorise UDP entrant (>1025)

```
hurricane:~# dmesg | grep 212
DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=80 TOS=0x00
   PREC=0x00 TTL=64 ID=6 DF PROTO=UDP SPT=1065 DPT=32769 LEN=60
DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=44 TOS=0x00
   PREC=0x00 TTL=64 ID=7 DF PROTO=UDP SPT=1065 DPT=32769 LEN=24
```

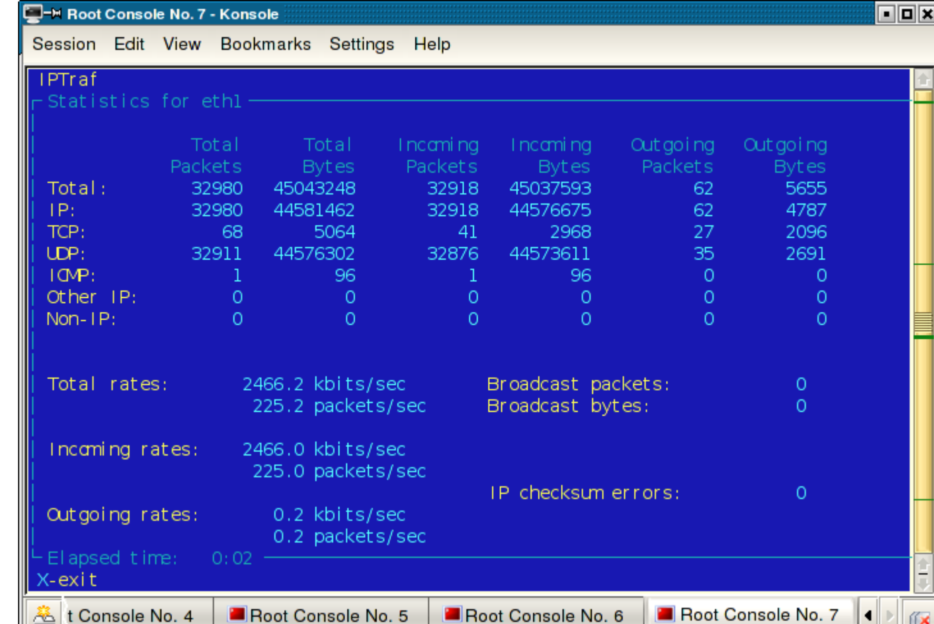
- Tiens, une émission sur les dinosaures...

- Les chaînes défilent toutes seules (?!?)

```
hurricane:~# dmesg | grep 212
DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=80 TOS=0x00
   PREC=0x00 TTL=64 ID=6 DF PROTO=UDP SPT=1065 DPT=32769 LEN=60
DROPPED IN= OUT=eth1 SRC=81.56.84.23 DST=212.27.38.253 LEN=44 TOS=0x00
   PREC=0x00 TTL=64 ID=7 DF PROTO=UDP SPT=1065 DPT=32769 LEN=24
```

- On autorise l'UDP sortant vers la plage 32000-33999
- « Ca marche. »

```
hurricane:~# dmesg | grep 212
hurricane:~# iptraf
hurricane:~#
```



- Au fait... la documentation !

Plan (2/2)

- Protection utilisées dans la pratique
  - Protection réseau et *firewall*
  - **Systèmes d'authentification**
  - Chiffrement de flux et VPN
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
  - Détection d'intrusion
  - Audit, tests d'intrusion
  - Administration, exploitation et suivi de la sécurité
  - Observation et surveillance
- Protection des applications usuelles

Authentification

- Codes d’accès (« Sésame, ouvre-toi ! »)
- Numéros (pistes ISO, codes barres, RFID, etc.)
- Nom d’utilisateur / mot de passe
- Clef publiques/clefs privés: RSA, DSA pour SSH, IKE, etc.
- Authentification forte des utilisateurs
  - S/Key
  - Mots de passe jetables
  - Cartes à puce et *token*
- …et les applications ?







Méthodes d'authentification

- Authentification locale
  - danger: divulgation du mot de passe en clair
    ⇒ chiffrement spécifique
- Défi réponse
  - défi: $\{aléa\}_{Ku}$ réponse: $\{aléa+1\}_{Ku}$
- Mots de passe jetables
- Systèmes cartes à puce (clé symétrique)
  - $K_{fille} = \{id\}_{K_{mère}}$
- Authentification « *zero knowledge* »

Le mot de passe

- C’est toujours la technique reine
- Elle combine l’identifiant (le nom d’utilisateur) et l’authentifiant (mot de passe secret)
- Cet authentifiant est stocké à disposition du système d’authentification
  - sous forme « obscurcie »
  - sous forme chiffrée
  - sous une forme chiffrée résistante
  - parfois en clair
- Ne pas confondre avec un(e) « *passphrase* »

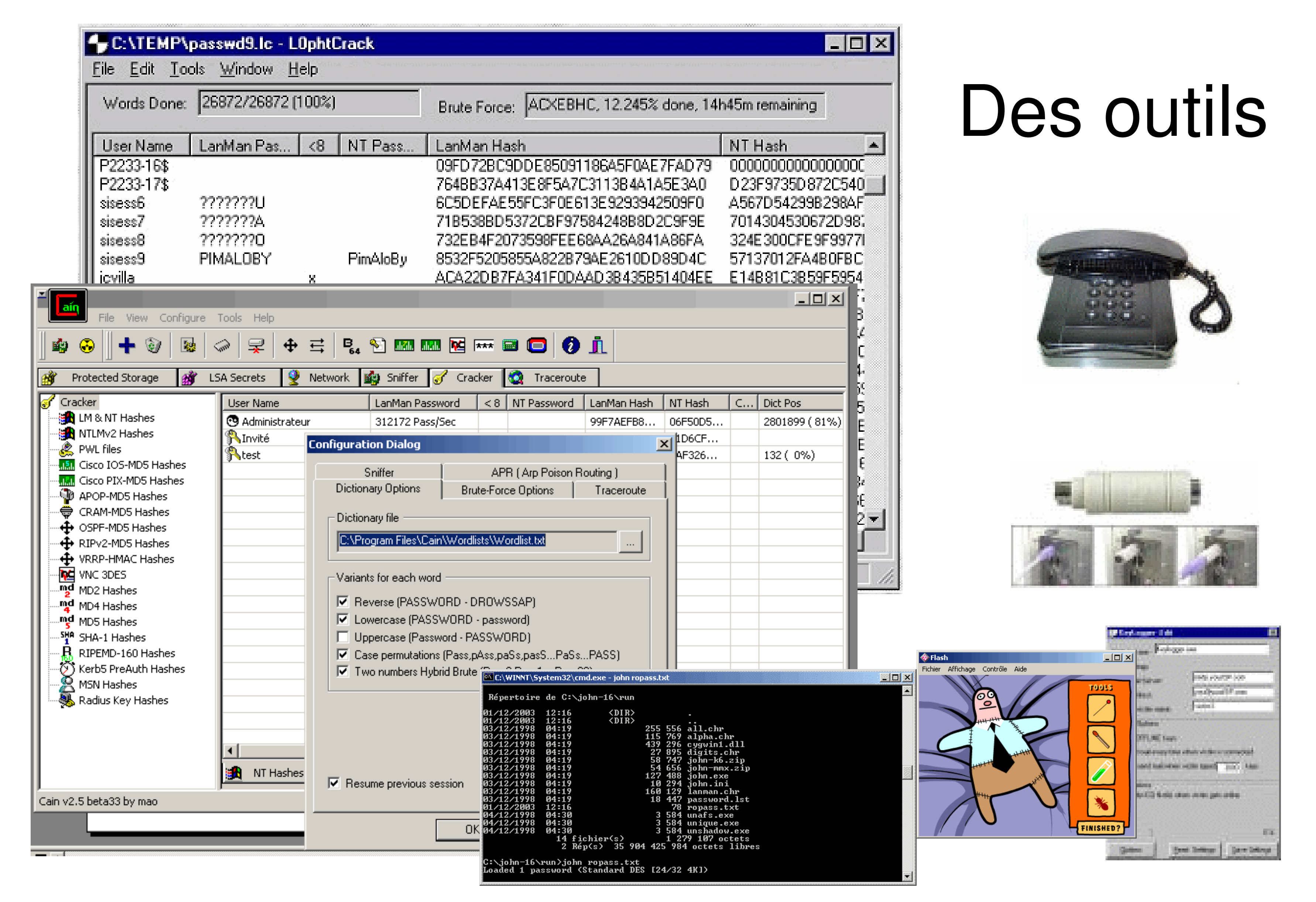
Un bon mot de passe

- Personnel
  spécifique à chaque individu
- Fiable
  durablement mémorisé
- Résistant
  qui ne soit pas facile à deviner pour un tiers

L’attaque des mots de passe

- Demander à l’utilisateur
- Dans la poubelle (ou sous le clavier)
- A la source (Cheval de Troie, enregistreur clavier)
- Inversion du codage
- Attaque par dictionnaire (*password cracking*)
  - Nécessite le vol de la forme stockée (chiffrée)
  - Essais successifs par rapport à un dictionnaire pré-établi
  - Prise en compte de règles de combinaison simples (à l’envers, ajout d’un ou deux chiffres)
  - La recherche exhaustive est accessibles sur les alphanumériques (avec une longueur limitée : 6 en général)
  - Surtout intéressant sur un ensemble de comptes
  - Forme directe d’une attaque générale (*codebook-based*)
  - Le choix du dictionnaire est important (prénoms, acronymes)

Des outils



> 10^6 $pass_{NT}$ / s

http://lasecpc13.epfl.ch/ntcrack/

Un bon mot de passe

- Utiliser une phrase (citation) relativement longue et peut-être personnelle
- Sélectionner les lettres (première, deuxième, dernière)

e o n p e t e l q

être ou ne pas être, telle est la question

u u p c r l e p e p
t n h i e o t e t e
Sll(p,d,d)

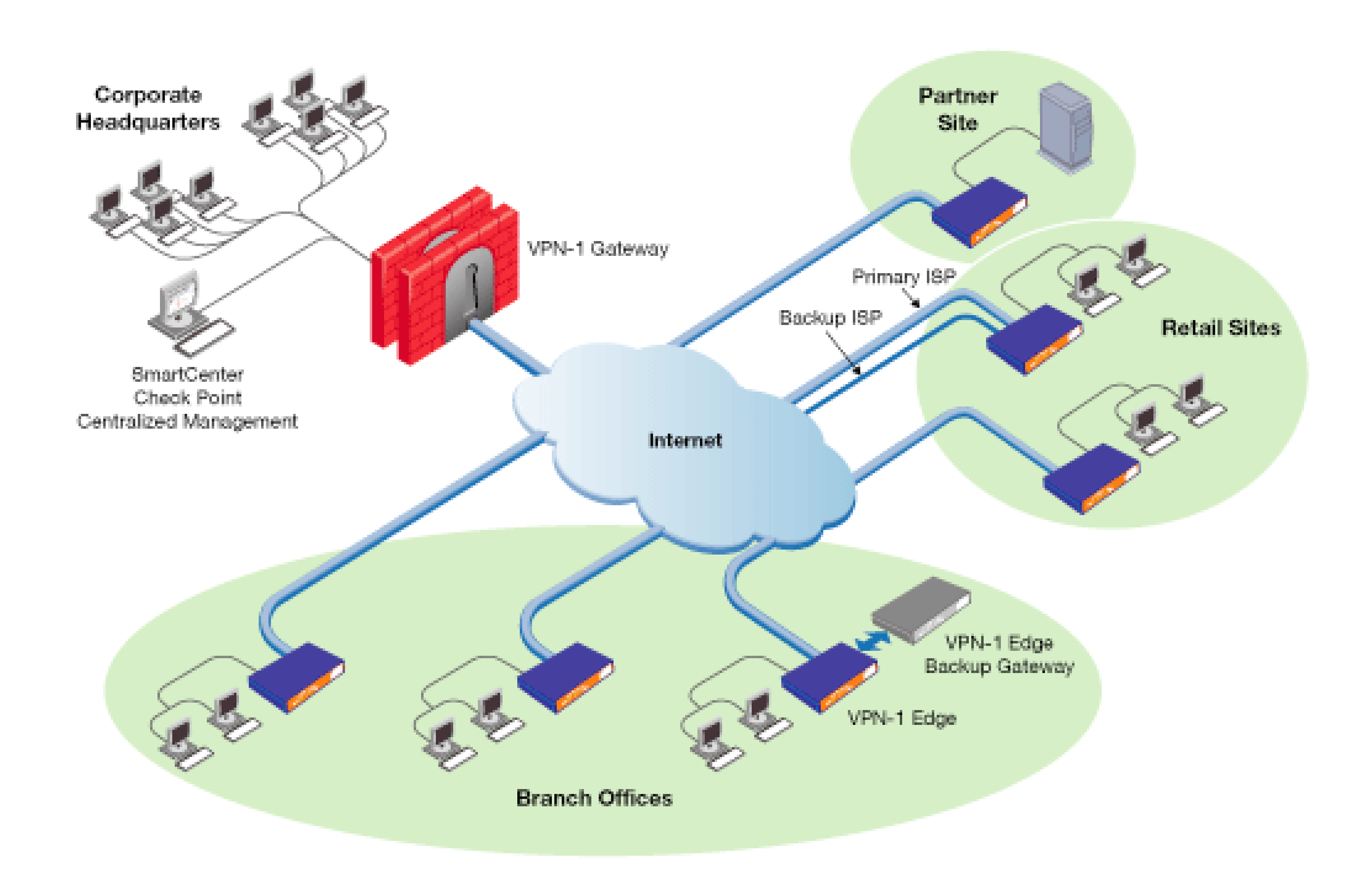
Plan (2/2)

- Protection utilisées dans la pratique
  - Protection réseau et *firewall*
  - Systèmes d'authentification
  - **Chiffrement de flux et VPN**
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
  - Détection d'intrusion
  - Audit, tests d'intrusion
  - Administration, exploitation et suivi de la sécurité
  - Observation et surveillance
- Protection des applications usuelles

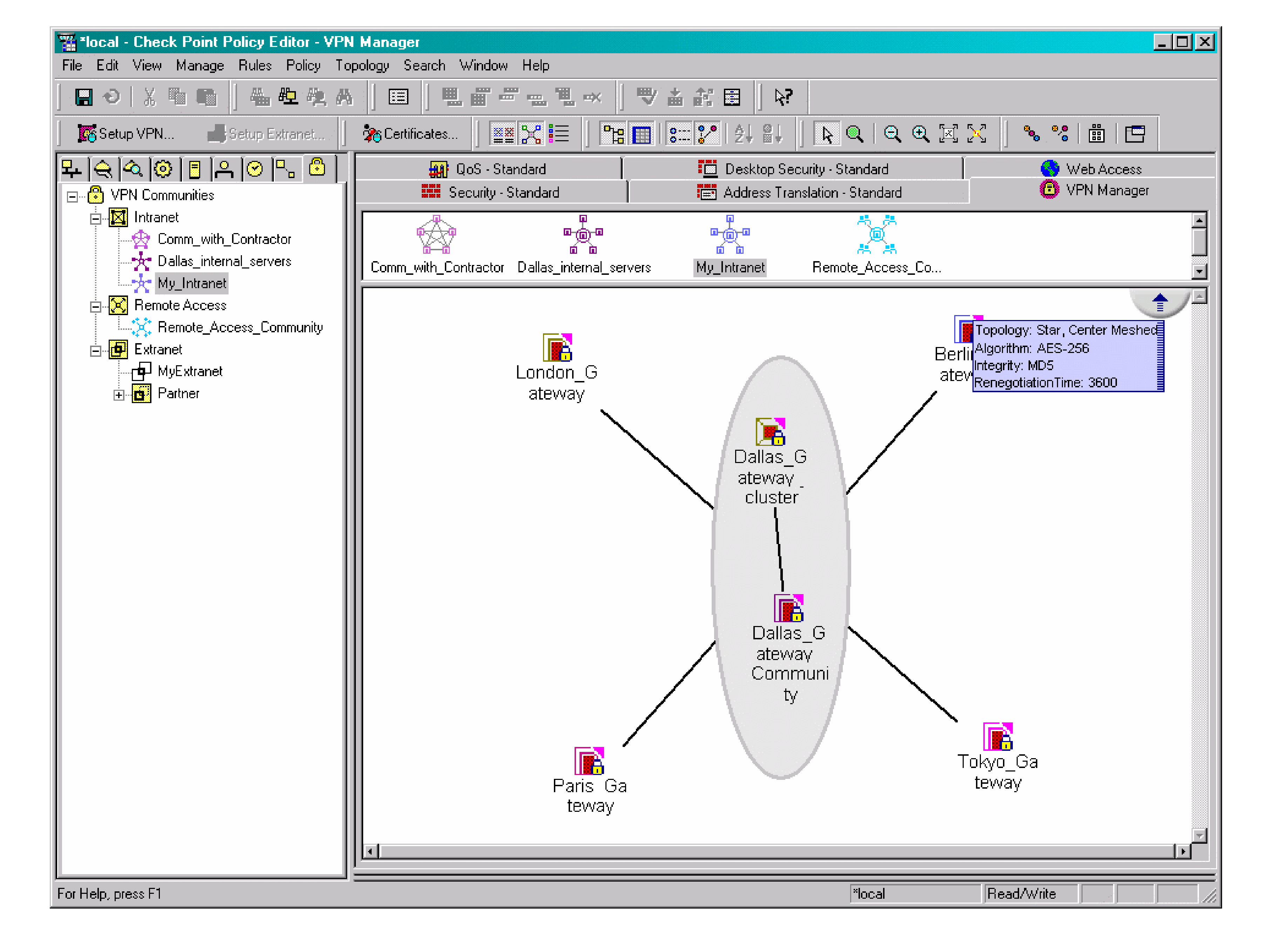
VPN

- IPSEC/IKE
  - Site à site (*gateway* ↔ *gateway*, *hosts* ↔ *hosts*)
  - Client à site (nomade, *host* ↔ *gateway*)
- SSH
- SSL (OpenVPN)
- Clients VPN « personnels » (authentification de l'utilisateur)
- Exemples de solutions commerciales

Ex. : CheckPoint VPN-1

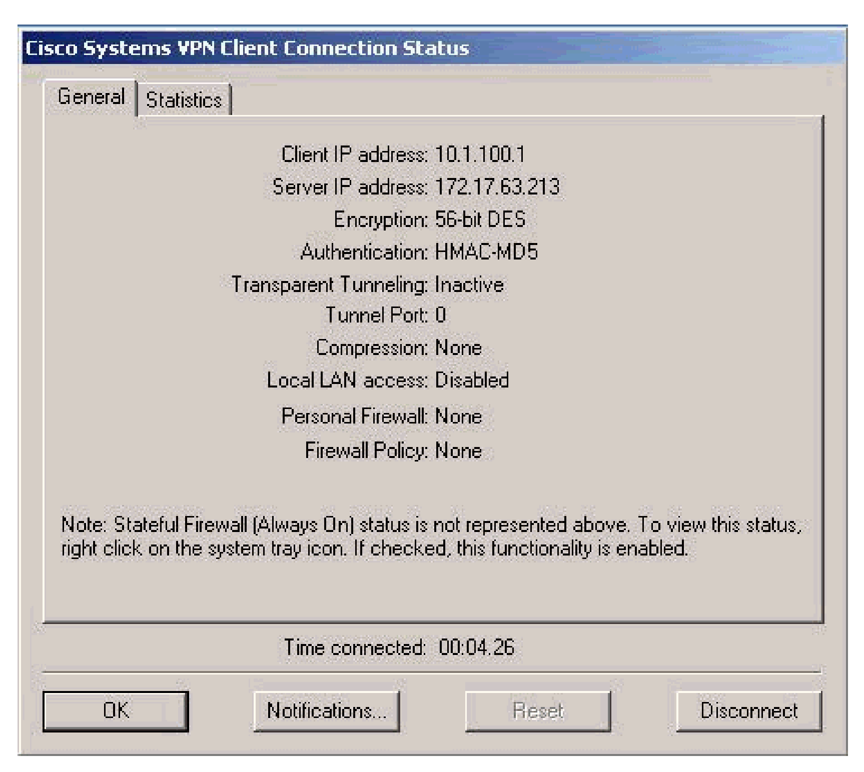


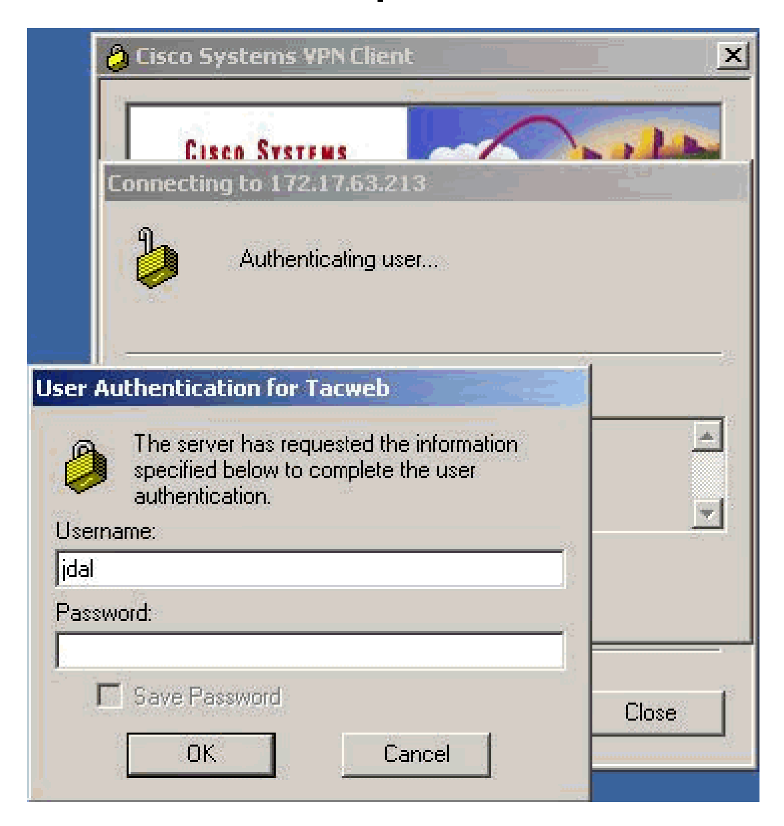
Ex. : CheckPoint VPN-1



IPSEC et X-AUTH

- Extension non-standard
- Sorte d'insertion d'une authentification de l'utilisateur par mot de passe (à la RADIUS) entre les deux phases IKE





SSL/TLS – IPSEC/IKE – HTTPS

- Utiliser des certificats plutôt que des mots de passe pour les tunnels VPN
- Générer si besoin ces certificats via `openssl` (réduire la gestion de clefs au minimum)
- X.509
- Ce genre d'action est toutefois préparatoire à la compréhension d'autres notions
  - Comment délivrer des certificats à tous les utilisateurs
  - Comment garantir un niveau de sécurité
  - Pour quoi faire : accès nomade, relevé de comptes bancaires, déclaration de revenu, et puis …

Plan (2/2)

- Protection utilisées dans la pratique
  - Protection réseau et *firewall*
  - Systèmes d'authentification
  - Chiffrement de flux et VPN
- **Digressions (RàZ, OpenBSD, 1984)**
- Surveiller, analyser et gérer
  - Détection d'intrusion
  - Audit, tests d'intrusion
  - Administration, exploitation et suivi de la sécurité
  - Observation et surveillance
- Protection des applications usuelles

Digressions

- How to 0wn the Internet in your spare time?
  - puis faire un RàZ
- OpenBSD
  - pas là par contre

http://www.openbsd.org/security.html

- 1984
  - et l'impact sur la vie réelle?

Plan (2/2)

- Protection utilisées dans la pratique
  - Protection réseau et *firewall*
  - Systèmes d'authentification
  - Chiffrement de flux et VPN
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
  - **Détection d'intrusion**
  - Audit, tests d'intrusion
  - Administration, exploitation et suivi de la sécurité
  - Observation et surveillance
- Protection des applications usuelles

Plan (détaillé)

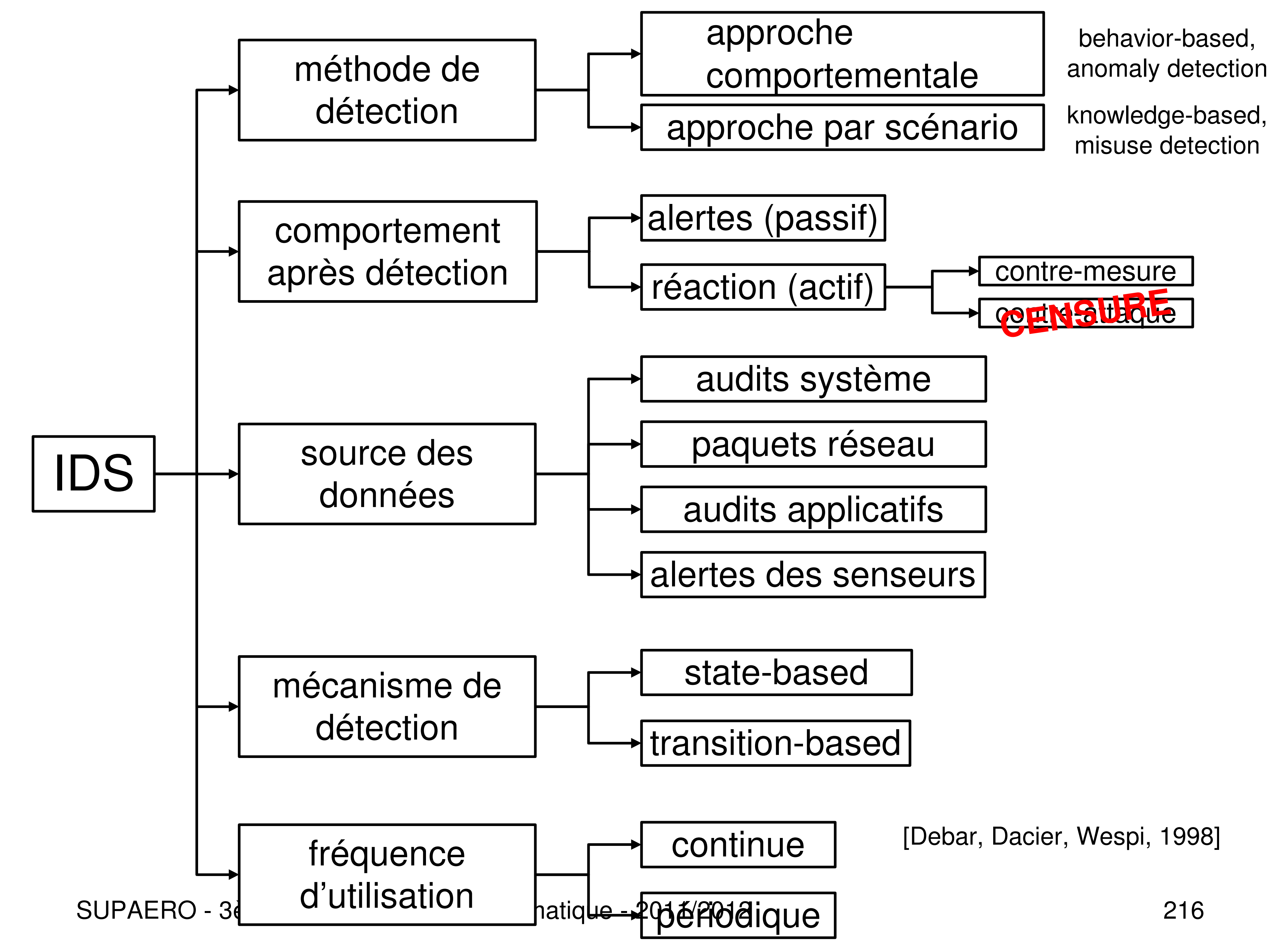
- **Détection d'intrusion**
  - Terminologie
  - Approches étudiées et tendances
  - Mise en oeuvre
  - Architecture
  - Solutions (réseau)
    - RealSecure
    - Snort
    - Prelude-IDS
  - Traitement des alertes (problèmes, corrélation)

Vulnérabilités – Attaques – Alertes

- Vulnérabilités
  - Grande variété : *buffer overflow*, CGI, droits d’accès permissifs, interception de sessions réseaux, transferts de privilèges, *social engineering*, cryptanalyse, etc.
- « Attaque »
  - Exploitation d’une vulnérabilité
  - Attaque élémentaire ou scénario d’intrusion
  - Action malveillante ou suspecte
- Alertes
  - Message résultant de la détection d’une attaque
  - *IDMEF (XML): Intrusion Detection Message Exchange Format défini par l’IETF/IDWG*

Génération d'alertes (efficacité)

	Pas d'alerte	Alerte
Pas d'attaque	Vrai négatif ☺	Faux positif ☹
Attaque en cours	Faux négatif ☹	Vrai positif 😐


IDS
méthode de détection
approche comportementale
behavior-based, anomaly detection
approche par scénario
knowledge-based, misuse detection
comportement après détection
alertes (passif)
réaction (actif)
contre-mesure
contre-attaque
CENSURE
source des données
audits système
paquets réseau
audits applicatifs
alertes des senseurs
mécanisme de détection
state-based
transition-based
fréquence d'utilisation
continue
périodique
[Debar, Dacier, Wespi, 1998]
SUPAERO - 3è
atique - 2011/2012

Techniques utilisables

- Approche par scénario
  - Systèmes experts (ES)
  - Analyse de signatures (SA)
  - Réseaux de Petri (PN)
- Approche comportementale
  - Statistiques (ST)
  - Systèmes experts (ES)
  - Réseaux neuronaux (NN)
  - Approche immunologique (UII)

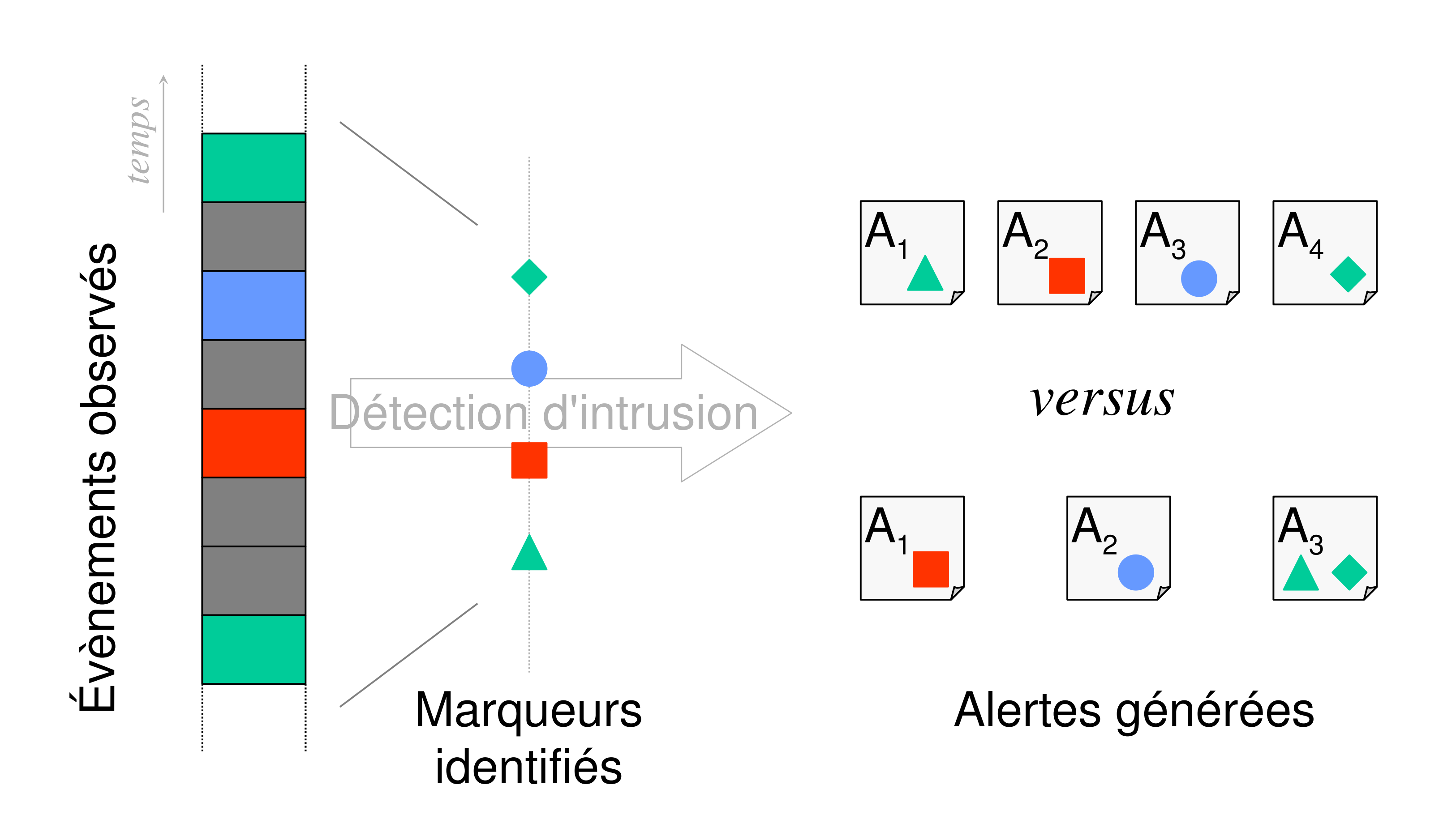
Beaucoup de techniques ont été explorées

Origine	Nom	Période	Hôte	Réseau	Scénario				Comportementale			
					ES	SA	PN	STA	ST	ES	NN	UII
Université de Namur	ASAX	1990-97	■		■							
AT&T	ComputerWatch	1987-90	■							■		
USAF	Haystack	1987-90	■						■			
	DIDS	1989-95	■	■	■				■			
CS Telecom	Hyperview	1990-95	■		■				■		■	
SRI	IDES	1983-92	■		■				■			
	NIDES	1992-95	■		■				■			
	Emerald	1996-		■		■			■			
Purdue University	IDIOT	1992-97	■				■	■				
U.C. Davis	NSM	1989-95		■		■			■			
	GrIDS	1995-		■						■		
LANL	W&S	1987-90	■							■		
	Nadir	1990-	■		■					■		
Cisco/WheelGroup	NetRanger	1995-		■		■						
ISS	RealSecure	1995-	■	■		■						
Securenet Consortium	SecureNet	1992-96	■		■				■		■	■
Network Associates Inc.	Stalker	1995-	■			■						
	WebStalker CyberCop Server	1997-	■							■		
U.C. Santa-Barbara (UCSB)	STAT	1991-92	■					■				
	USTAT	1992-93	■					■				
Stanford University	Swatch	1992-93	■		■							
MCNC et NCSU	JiNao	1995-		■	■				■			

Tendances actuelles

- Une seule technique par outil en général
- L'approche par signatures se généralise
  - Réalisation plus simple
  - Performances
- L'approche comportementale est peu utilisée par les outils commerciaux
- La réaction apparaît

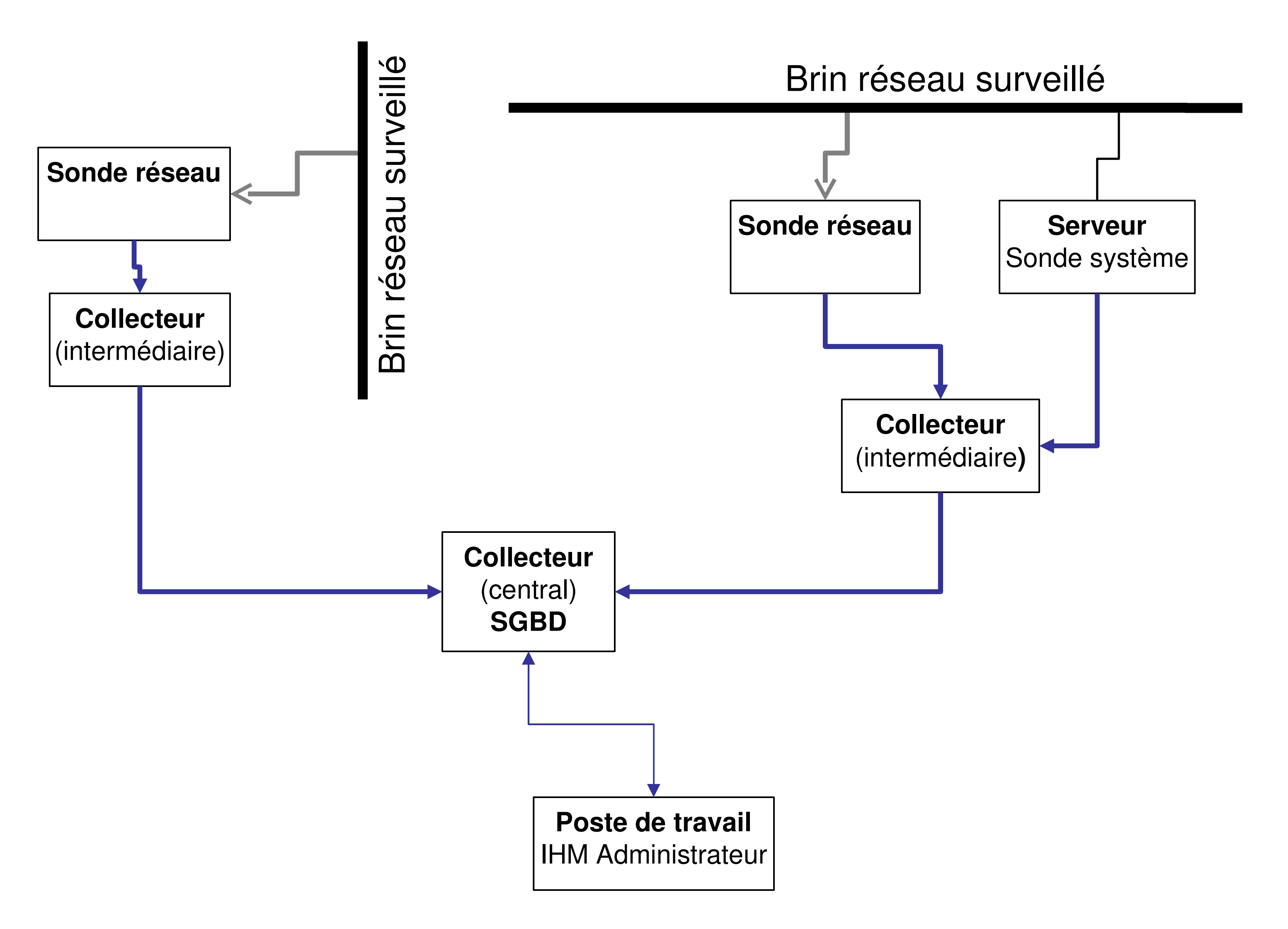
Analyse multi-évènements



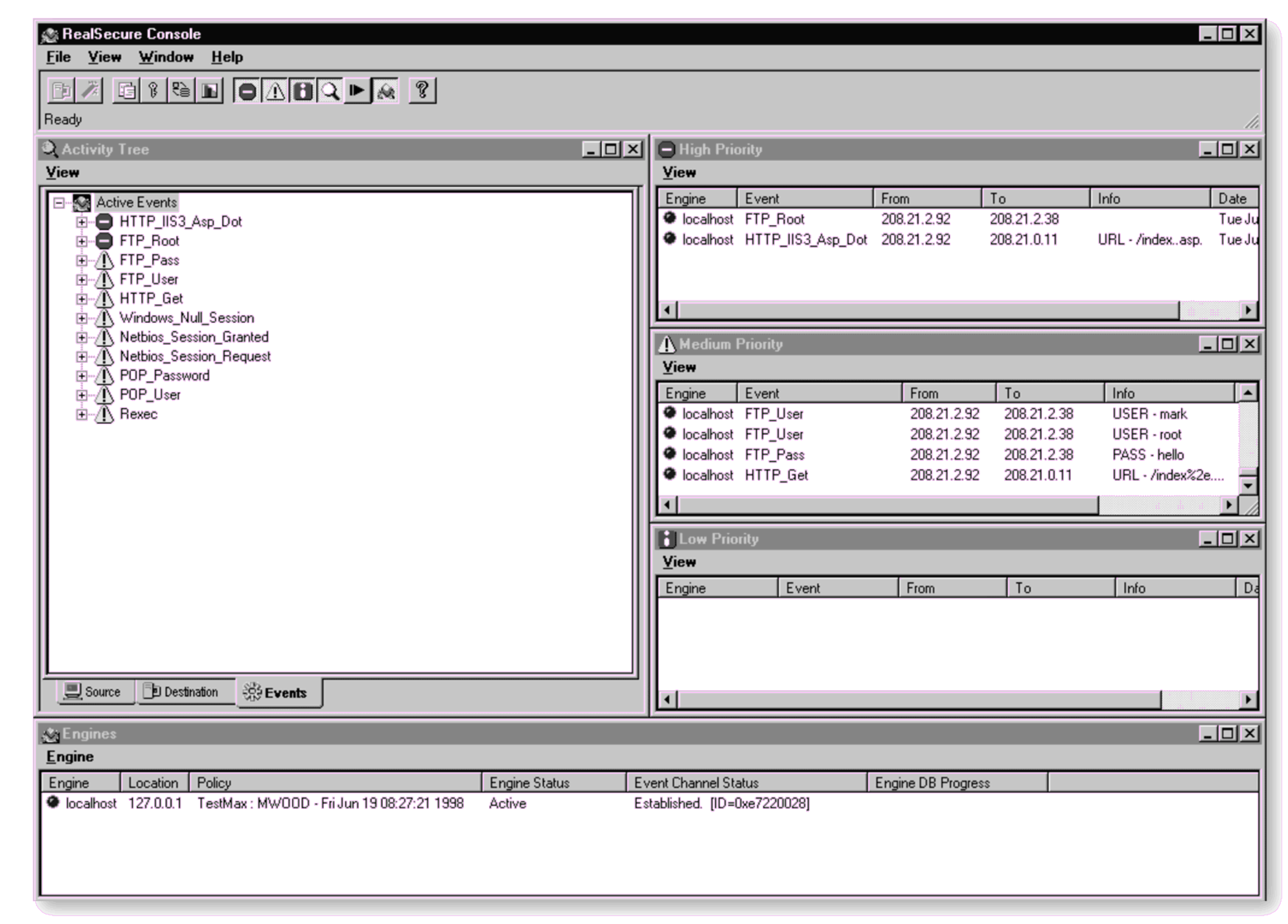
Mise en oeuvre

- Sondes
  - Observation du trafic
    - Positionnement
    - Problème des environnements commutés (*mirroring* vs. *taps*)
  - Sondes système
  - Nombre des signatures (et impact CPU)
  - Pertinence des signatures
- Consolidation des alertes
  - Collecteurs
  - Protocole d'échange sécurisé
  - Format d'échange IDMEF: http://www.ietf.org/html.charters/idwg-charter.html

Architectures envisageables



Ex. : IHM ISS RealSecure

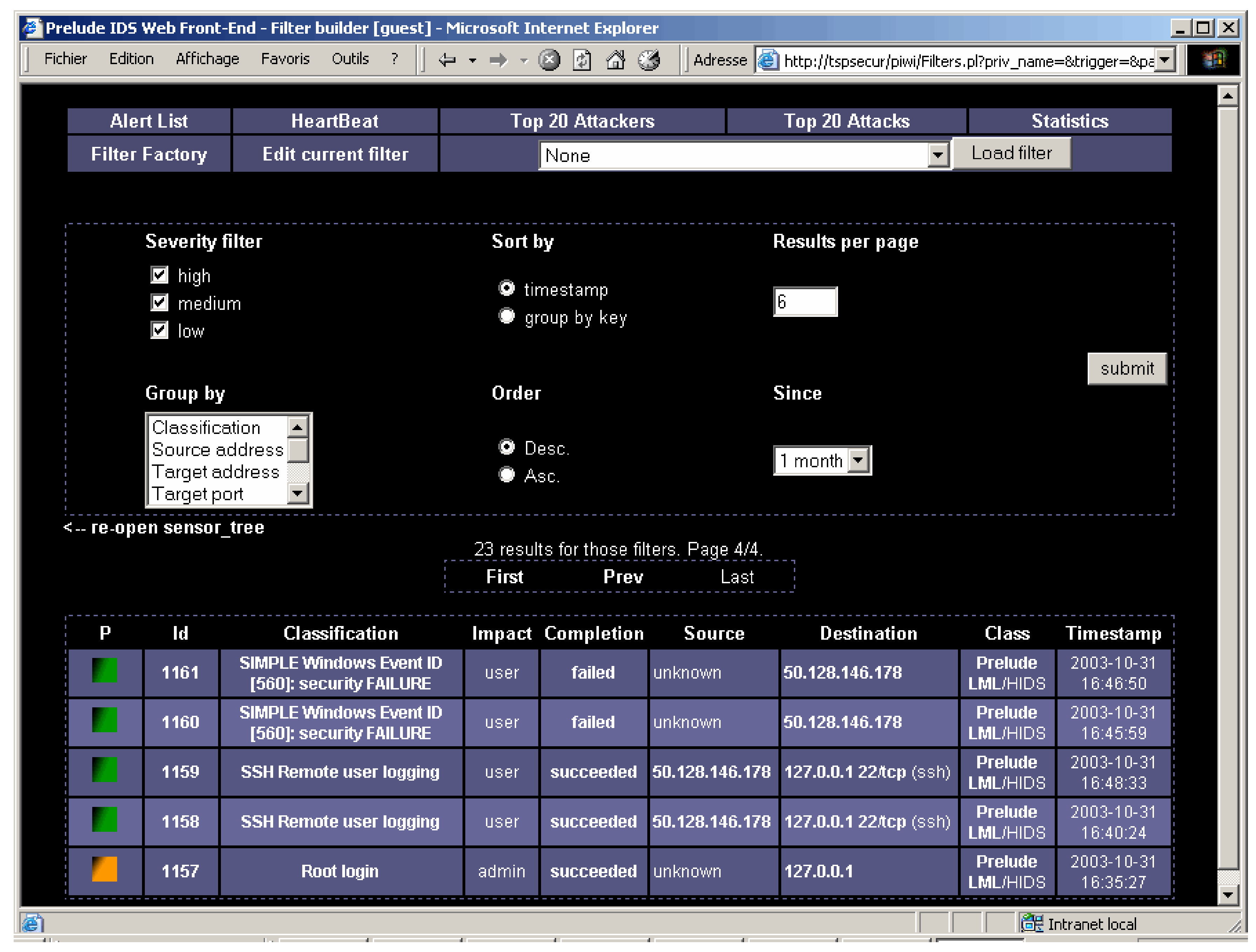


Signatures – Snort (1)

SID	1800
Message	VIRUS Klez Incoming
Signature	alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"VIRUS Klez Incoming"; flow:to_server,established; dsize:>120; content:"MIME"; content:"VGhpcyBwcm9"; classtype:misc-activity; sid:1800; rev:3;)
Summary	This event is generated when an incoming email containing the Klez worm is detected.
Impact	System compromise and further infection of target hosts.
Detailed Information	W32/Klez.h@MM exploits the vulnerability in Microsoft Internet Explorer (ver 5.01 or 5.5 without SP2), enabling it to execute email attachments. Once executed, it can unload several processes including Anti-virus programs. The worm is able to propagate over the network by copying itself to network shares (assuming sufficient permissions exist). Target filenames are chosen randomly, and can have single or double file extensions.
Affected Systems	Microsoft Internet Explorer (ver 5.01 or 5.5 without SP2)
Attack Scenarios	This virus can be considered a blended threat. It mass-mails itself to email addresses found on the local system, then exploits a known vulnerability, spreads via network shares, infects executables on the local system.
Ease of Attack	Simple. This is worm activity.
False Positives	Certain binary file email attachments can trigger this alert.
False Negatives	None known.
Corrective Action	Apply the appropriate vendor suppled patches. Block incoming attachments with .bat, .exe, .pif, and .scr extensions
Contributors	Sourcefire Research Team Brian Caswell <bmc@sourcefire.com>

Signatures – Snort (2)

SID	2251
Message	NETBIOS DCERPC Remote Activation bind attempt
Signature	alert tcp $EXTERNAL_NET any -> $HOME_NET 135 (msg:"NETBIOS DCERPC Remote Activation bind attempt"; content:"|05|"; distance:0; within:1; content:"|0b|"; distance:1; within:1; byte_test:1,&,1,0,relative; content:"|B8 4A 9F 4D 1C 7D CF 11 86 1E 00 20 AF 6E 7C 57|"; distance:29; within:16; reference:cve,CAN-2003-0352; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/bulletin/MS03-026.asp; reference:cve,CAN-2003-0715; sid:2251; rev:1;)
Summary	This event is generated when an attempt is made to exploit a known vulnerablity in Microsoft RPCSS service for RPC.
Impact	Denial of Service. Possible execution of arbitrary code leading to unauthorized remote administrative access.
Detailed Information	A vulnerability exists in Microsoft RPCSS Service that handles RPC DCOM requests such that execution of arbitrary code or a Denial of Service condition can be issued against a host by sending malformed data via RPC. The Distributed Component Object Model (DCOM) handles DCOM requests sent by clients to a server using RPC. A malformed request to the host running the RPCSS service may result in a buffer overflow condition that will present the attacker with the opportunity to execute arbitrary code with the privileges of the local system account. Alternatively the attacker could also cause the RPC service to stop answering RPC requests and thus cause a Denial of Service condition to occur.
Affected Systems	Windows NT 4.0 Workstation and Server Windows NT 4.0 Terminal Server Edition Windows 2000 Windows XP


Prelude IDS Web Front-End - Filter builder [guest] - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Adresse http://tspsecur/piwi/Filters.pl?priv_name=&trigger=&pa
Alert List
HeartBeat
Top 20 Attackers
Top 20 Attacks
Statistics
Filter Factory
Edit current filter
None
Load filter
Severity filter
high
medium
low
Sort by
timestamp
group by key
Results per page
6
submit
Group by
Classification
Source address
Target address
Target port
Order
Desc.
Asc.
Since
1 month
<-- re-open sensor_tree
23 results for those filters. Page 4/4.
First
Prev
Last
P
Id
Classification
Impact
Completion
Source
Destination
Class
Timestamp
1161
SIMPLE Windows Event ID [560]: security FAILURE
user
failed
unknown
50.128.146.178
Prelude LML/HIDS
2003-10-31 16:46:50
1160
SIMPLE Windows Event ID [560]: security FAILURE
user
failed
unknown
50.128.146.178
Prelude LML/HIDS
2003-10-31 16:45:59
1159
SSH Remote user logging
user
succeeded
50.128.146.178
127.0.0.1 22/tcp (ssh)
Prelude LML/HIDS
2003-10-31 16:48:33
1158
SSH Remote user logging
user
succeeded
50.128.146.178
127.0.0.1 22/tcp (ssh)
Prelude LML/HIDS
2003-10-31 16:40:24
1157
Root login
admin
succeeded
unknown
127.0.0.1
Prelude LML/HIDS
2003-10-31 16:35:27
Intranet local

Limites actuelles de la détection d'intrusion

- Faible taux de détection
  - Faux négatifs
- Trop d'alertes
  - Fausses alertes : Faux positifs
  - Plusieurs milliers d'alertes générées en une semaine
- Le niveau de granularité d'une alerte est trop faible
  - Pas de vision globale
  - Difficile de détecter une attaque distribuée
- Difficile de détecter les attaques nouvelles
  - C'est un avantage des approches comportementales

Granularité trop fine

Exemple : alertes générées par Dragon

[**] [1:1256:2] WEB-IIS CodeRed v2 root.exe access [**]
07/20-13:59:32.291193 64.165.187.170:4515 -> 193.54.194.111:80
[**] [1:1
07/20-1
[**] [1:1
07/20-1

SID	1256
Message	WEB-IIS CodeRed v2 root.exe access
Signature	alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS CodeRed v2 root.exe access"; flow:to_server,established; uricontent:"/root.exe"; nocase; classtype:web-application-attack; reference:url,www.cert.org/advisories/CA-2001-19.html; sid:1256; rev:7;)

[**] [1:1002:2] WEB-IIS cmd.exe access [**]
07/20-13:59:33.969027 64.165.187.170:4582 -> 193.54.194.111:80
[**] [1:1288:2] WEB-FRONTPAGE /_vti_bin/ access [**]
07/20-13:59:34.434017 64.165.187.170:4587 -> 193.54.194.111:80
[**] [1:1002:2] WEB-IIS cmd.exe access [**]
07/20-13:59:34.817953 64.165.187.170:4593 -> 193.54.194.111:80
[**] [1:1002:2] WEB-IIS cmd.exe access [**]
07/20-13:59:35.219711 64.165.187.170:4601 -> 193.54.194.111:80
[**] [1:1
07/20-1
[**] [1:1
07/20-1

SID	1002
Message	WEB-IIS cmd.exe access
Signature	alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS cmd.exe access"; flow:to_server,established; content:"cmd.exe"; nocase; classtype:web-application-attack; sid:1002; rev:5;)

Granularité trop fine

Exemple : alertes générées par Dragon

.

[**] [1:1256:2] WEB-IIS CodeRed v2 root.exe access [**]
07/20-13:59:32.291193 64.165.187.170:4515 -> 193.54.194.111:80
[**] [1:1002:2] WEB-IIS cmd.exe access [**]
07/20-13:59:33.059882 64.165.187.170:4533 -> 193.54.194.111:80
[**] [1:1002:
07/20-13:59
[**] [1:1002:
07/20-13:59
[**] [1:1288:
07/20-13:59:34.434017 64.165.187.170:4587 -> 193.54.194.111:80
[**] [1:1002:2] WEB-IIS cmd.exe access [**]
07/20-13:59:34.817053 64.165.187.170:4598 -> 193.54.194.111:80
[**] [1:1002:2] WEB-IIS cmd.exe access [**]
07/20-13:59:35.219711 64.165.187.170:4601 -> 193.54.194.111:80
[**] [1:1002:2] WEB-IIS cmd.exe access [**]
07/20-13:59:35.607048 64.165.187.170:4603 -> 193.54.194.111:80
[**] [1:1002:2] WEB-IIS cmd.exe access [**]
07/20-13:59:35.607048 64.165.187.170:4603 -> 193.54.194.111:80

.

Attaque *Nimda* de 64.165.187.170 vers 193.54.194.111

Sémantique trop pauvre

Exemple : alertes générées par Dragon

.

[**] [1:1256:2] WEB-IIS CodeRed v2 root.exe access [**]
07/20-13:59:32.291193 64.165.187.170:4515 -> 193.54.194.111:80
[**] [1:1002:2] WEB-IIS cmd.exe access [**]
07/20-13:59:33.059882 64.165.187.170:4533 -> 193.54.194.111:80
[**] [1:1002:
07/20-13:59
[**] [1:1002:
07/20-13:59
[**] [1:1288:
07/20-13:59
[**] [1:1002:
07/20-13:59:34.817053 64.165.187.170:459[illegible] -> 193.54.194.111:80
[**] [1:1002:2] WEB-IIS cmd.exe access [**]
07/20-13:59:35.219711 64.165.187.170:4601 -> 193.54.194.111:80
[**] [1:1002:2] WEB-IIS cmd.exe access [**]
07/20-13:59:35.607048 64.165.187.170:4603 -> 193.54.194.111:80
[**] [1:1002:2] WEB-IIS cmd.exe access [**]
07/20-13:59:35.607048 64.165.187.170:4603 -> 193.54.194.111:80

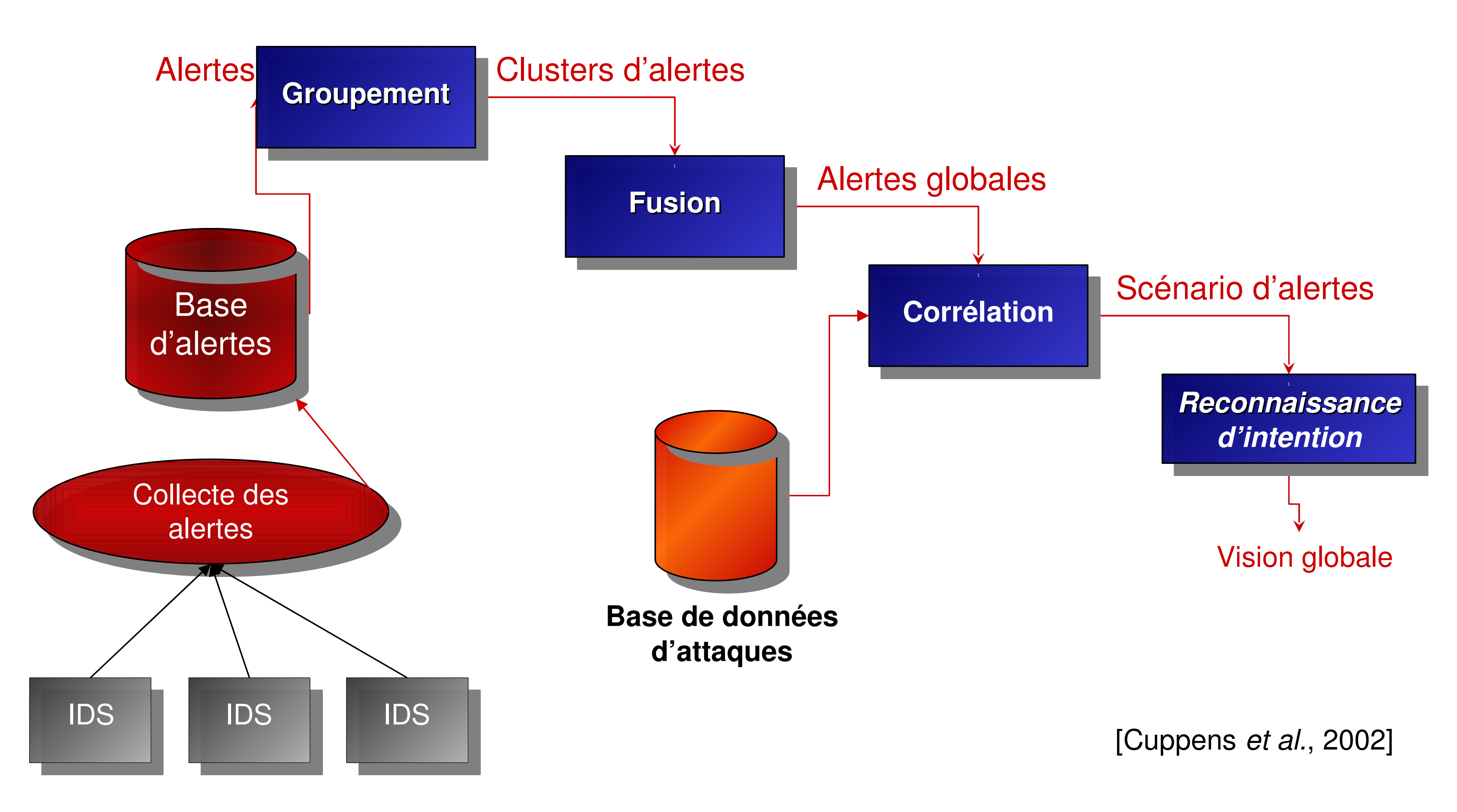
.

Attaque *Nimda* de 64.165.187.170 vers 193.54.194.111, 193.54.194.111 non-vulnérable

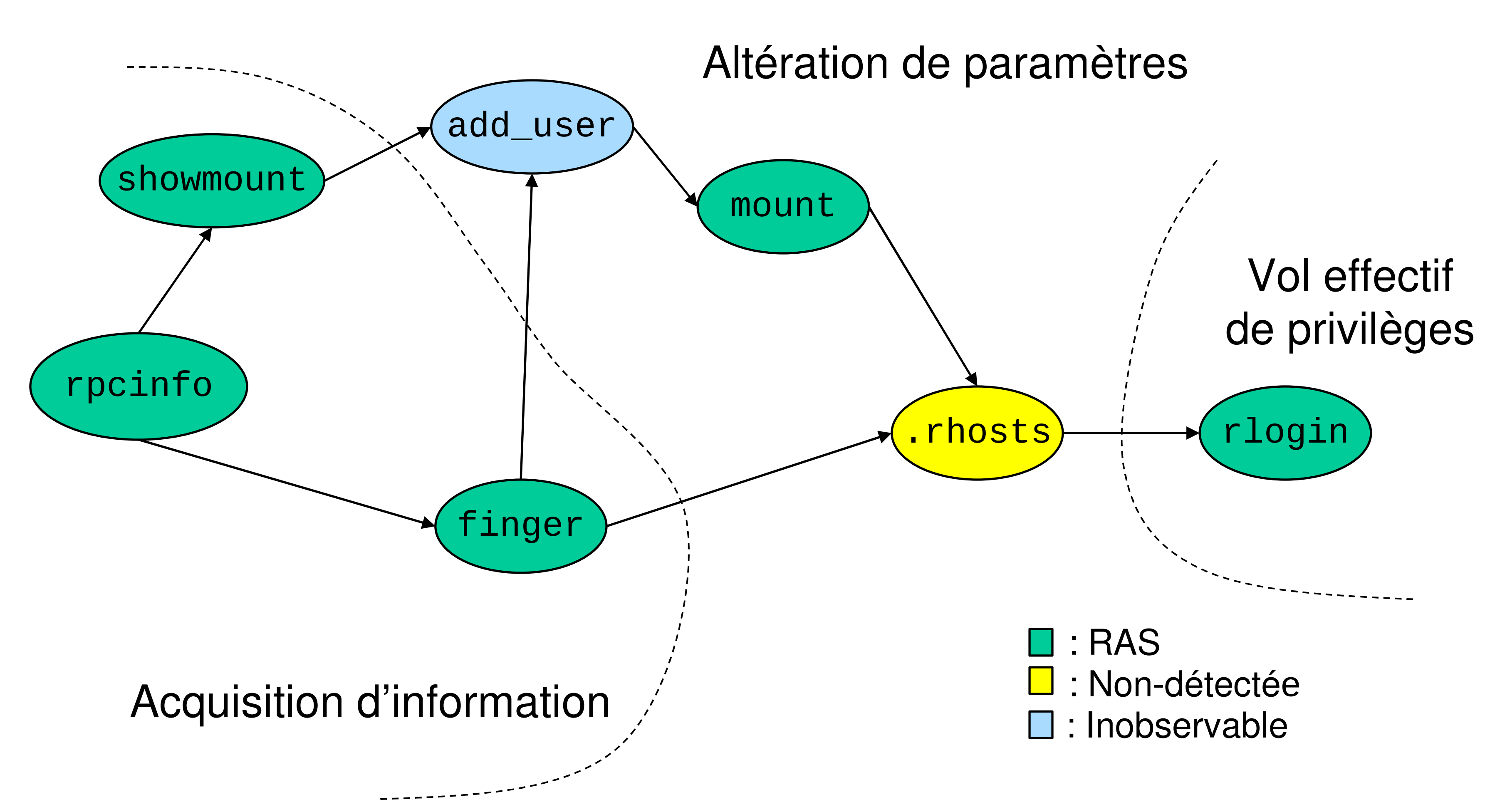
Corrélation d'alertes

- Développement des méthodes utilisables pour la corrélation
- Prise en compte d'information de cartographie
- Intégration de notions de groupement puis de fusion dans des outils existants ?

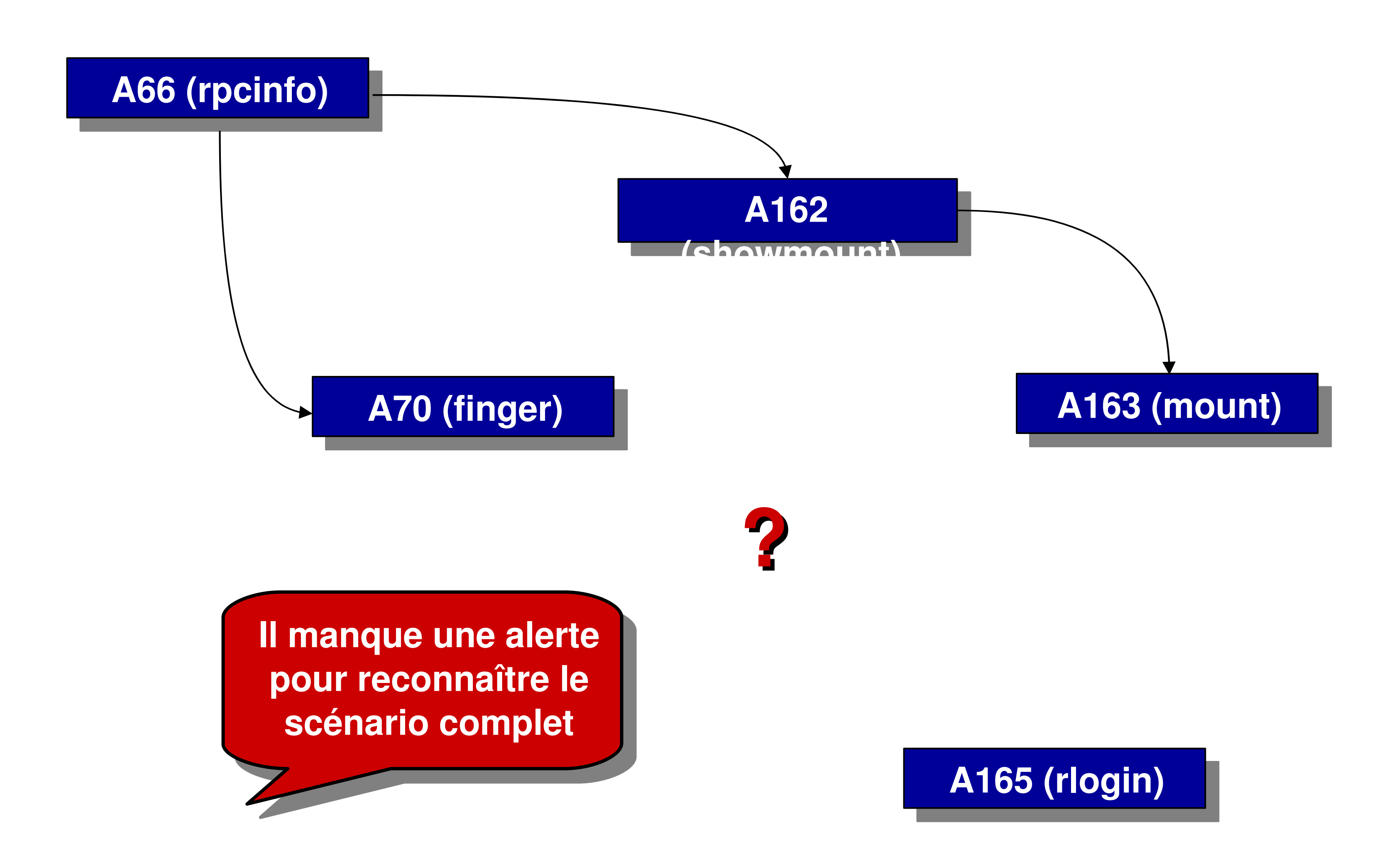
Les étapes du diagnostic



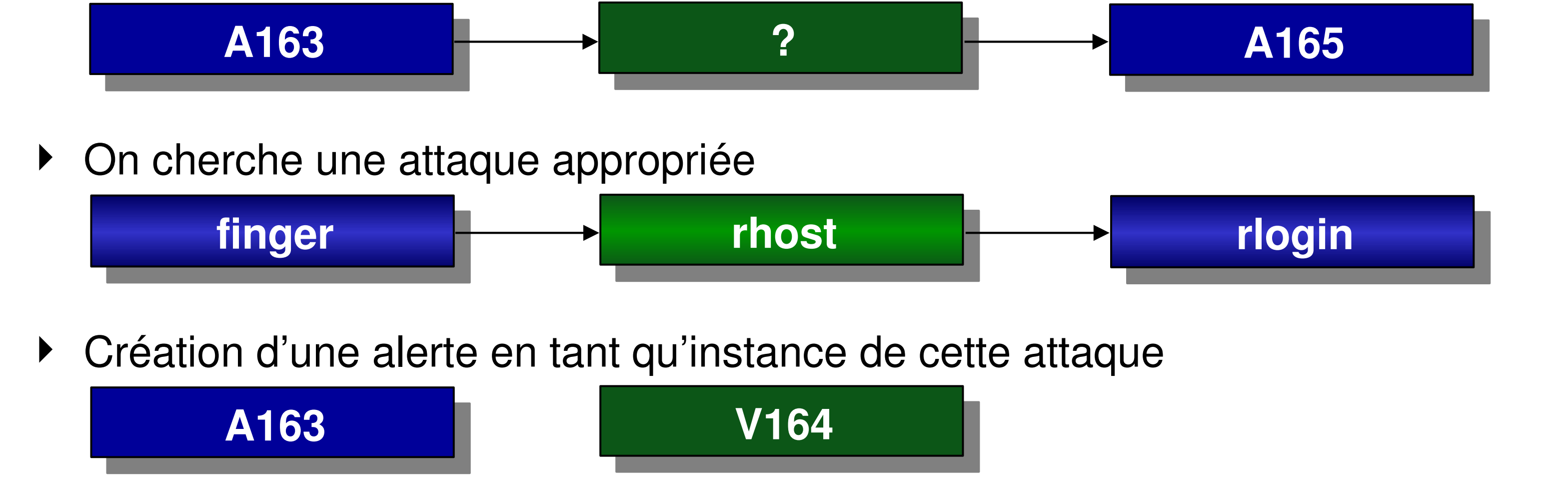
Scénario non-linéaire (exemple)



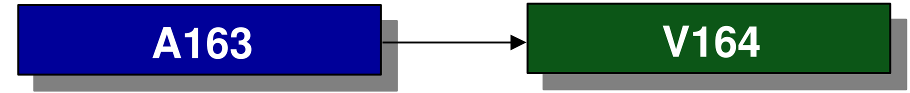
Exemple de corrélation



Génération d'hypothèse



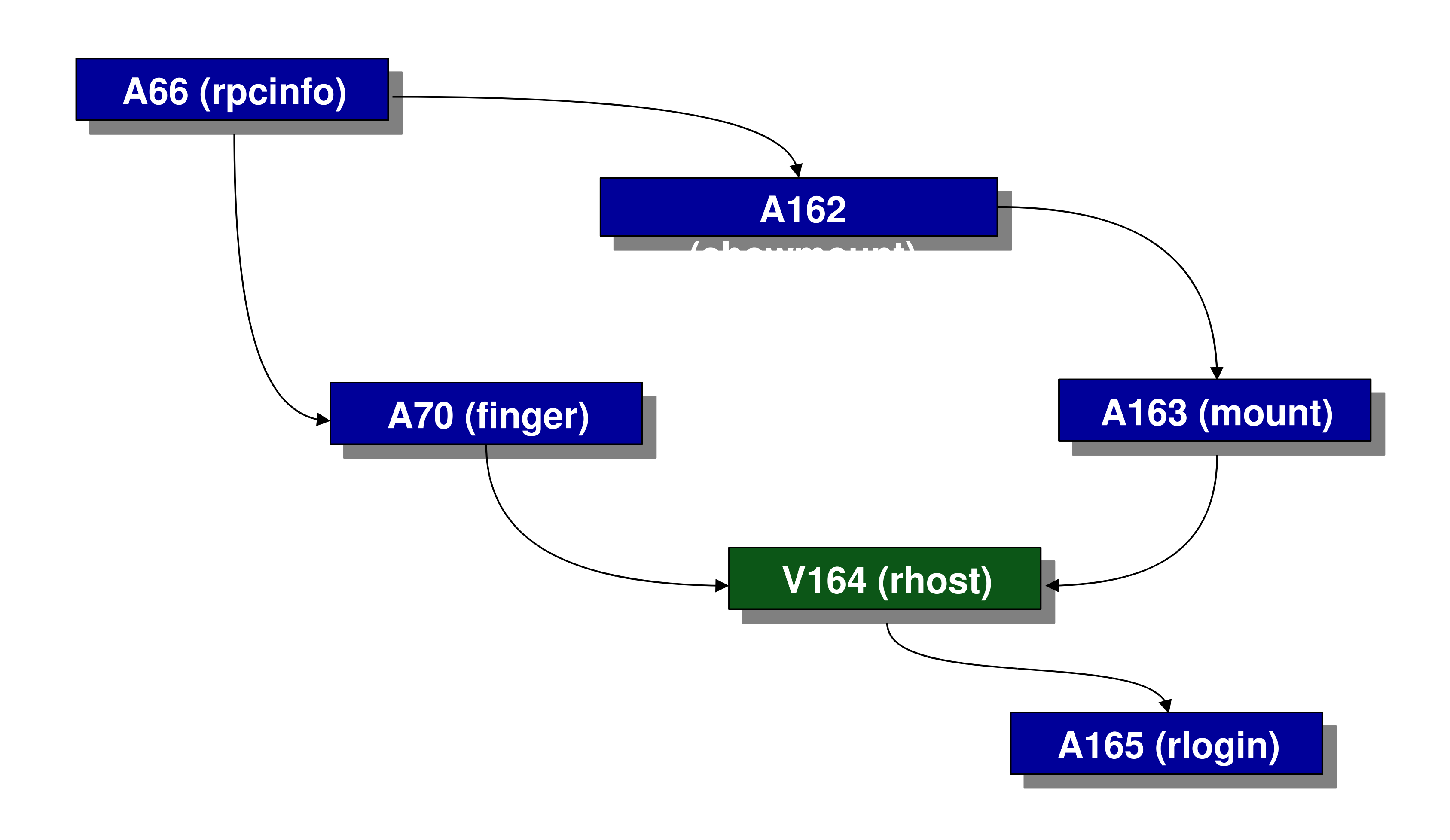
- On cherche une attaque appropriée
- Création d'une alerte en tant qu'instance de cette attaque
- Initialisation des champs de l'alerte grâce aux règles de corrélation



- Tentative de corrélation des deux dernières alertes



Résultat de la génération d’hypothèses



Plan (2/2)

- Protection utilisées dans la pratique
  - Protection réseau et *firewall*
  - Systèmes d’authentification
  - Chiffrement de flux et VPN
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
  - Détection d’intrusion
  - **Audit, tests d’intrusion**
  - Administration, exploitation et suivi de la sécurité
  - Observation et surveillance
- Protection des applications usuelles

Tests d'intrusion externes

- Une prestation assez répandue
- Avantages
  - Indépendance des acteurs
  - Bien délimitée
- Inconvénients
  - Ponctuelle
  - Limitée au périmètre accessible (Internet, infrastructure sécurité)
  - Dé-corrélée de la politique de sécurité
- Similaire à une simulation d'attaque

Outils d’audit

- Analyse active des vulnérabilités présentes
  - Plus ou moins agressif
  - Automatisation d’un test d’intrusion
  - Suivi
- Principaux produits existant
  - Nessus (*free software*)
  - ISS Internet Scanner
  - …

Nessus (1)

- Compilation et/ou installation (serveur, client)
- Création d'un utilisateur pour le serveur

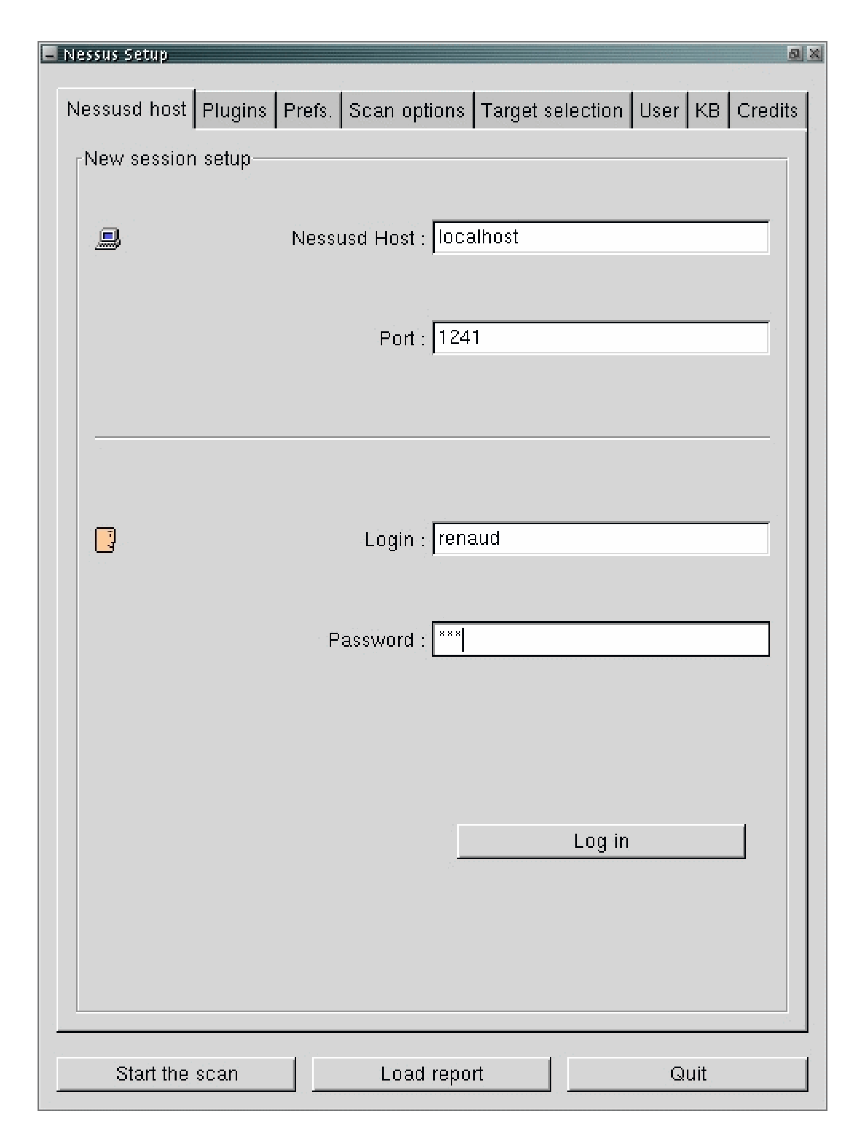
  `# nessus-adduser`

  - Authentification par certificat ou mot de passe
- Configuration

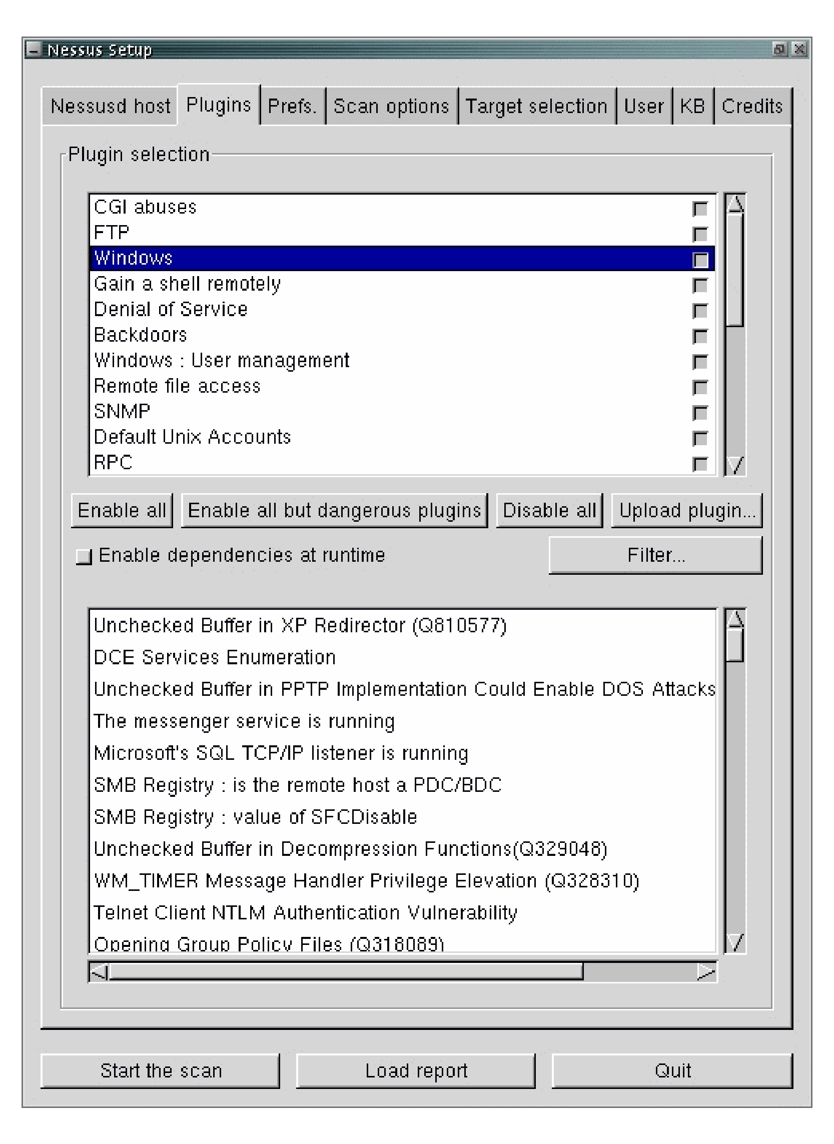
  `vi /usr/local/etc/nessus/nessusd.conf`
- Démarrage du démon

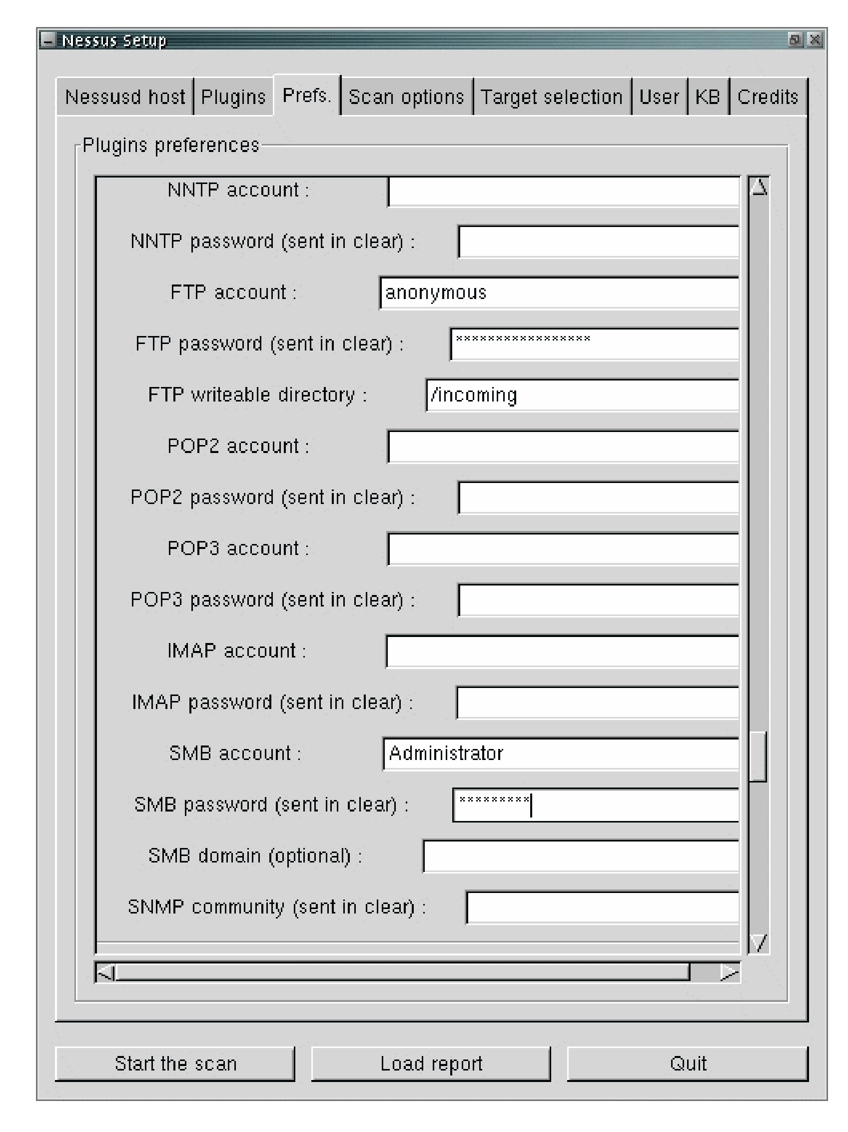
  `# nessusd -D`

  ou `/etc/init.d/nessusd start`
- Lancer le client



Nessus (2)


Nessus Setup
Nessusd host
Plugins
Prefs.
Scan options
Target selection
User
KB
Credits
Plugin selection
CGI abuses
FTP
Windows
Gain a shell remotely
Denial of Service
Backdoors
Windows : User management
Remote file access
SNMP
Default Unix Accounts
RPC
Enable all
Enable all but dangerous plugins
Disable all
Upload plugin...
Enable dependencies at runtime
Filter...
Unchecked Buffer in XP Redirector (Q810577)
DCE Services Enumeration
Unchecked Buffer in PPTP Implementation Could Enable DOS Attacks
The messenger service is running
Microsoft's SQL TCP/IP listener is running
SMB Registry : is the remote host a PDC/BDC
SMB Registry : value of SFCDisable
Unchecked Buffer in Decompression Functions(Q329048)
WM_TIMER Message Handler Privilege Elevation (Q328310)
Telnet Client NTLM Authentication Vulnerability
Opening Group Policy Files (Q318089)
Start the scan
Load report
Quit


Nessus Setup
Nessusd host
Plugins
Prefs.
Scan options
Target selection
User
KB
Credits
Plugins preferences
NNTP account :
NNTP password (sent in clear) :
FTP account :
anonymous
FTP password (sent in clear) :
FTP writeable directory :
/incoming
POP2 account :
POP2 password (sent in clear) :
POP3 account :
POP3 password (sent in clear) :
IMAP account :
IMAP password (sent in clear) :
SMB account :
Administrator
SMB password (sent in clear) :
SMB domain (optional) :
SNMP community (sent in clear) :
Start the scan
Load report
Quit

Nessus (3)

Nessus Setup

Nessusd host | Plugins | Prefs. | Scan options | Target selection | User | KB | Credits

Target selection

Target(s) : 10.163.156.0-10.163.156.254 [Read file...]

☐ Perform a DNS zone transfer

☐ Save this session

☐ Save empty sessions

Previous sessions :

Session	Targets

[Restore session] [Delete session]

[Start the scan] [Load report] [Quit]

Nessus Setup

Nessusd host | Plugins | Prefs. | Scan options | Target selection | User | KB | Credits

Scan options

Port range : 1-1500

☐ Consider unscanned ports as closed

Number of hosts to test at the same time : 10

Number of checks to perform at the same time : 10

Path to the CGIs : /cgi-bin:/scripts

☐ Do a reverse lookup on the IP before testing it

☐ Optimize the test

☐ Safe checks

☐ Designate hosts by their MAC address

☐ Detached scan

Send results to this email address :

☐ Continuous scan

Delay between two scans :

Port scanner :

tcp connect() scan

Nmap

scan for LaBrea tarpitted hosts

SYN Scan

[Start the scan] [Load report] [Quit]

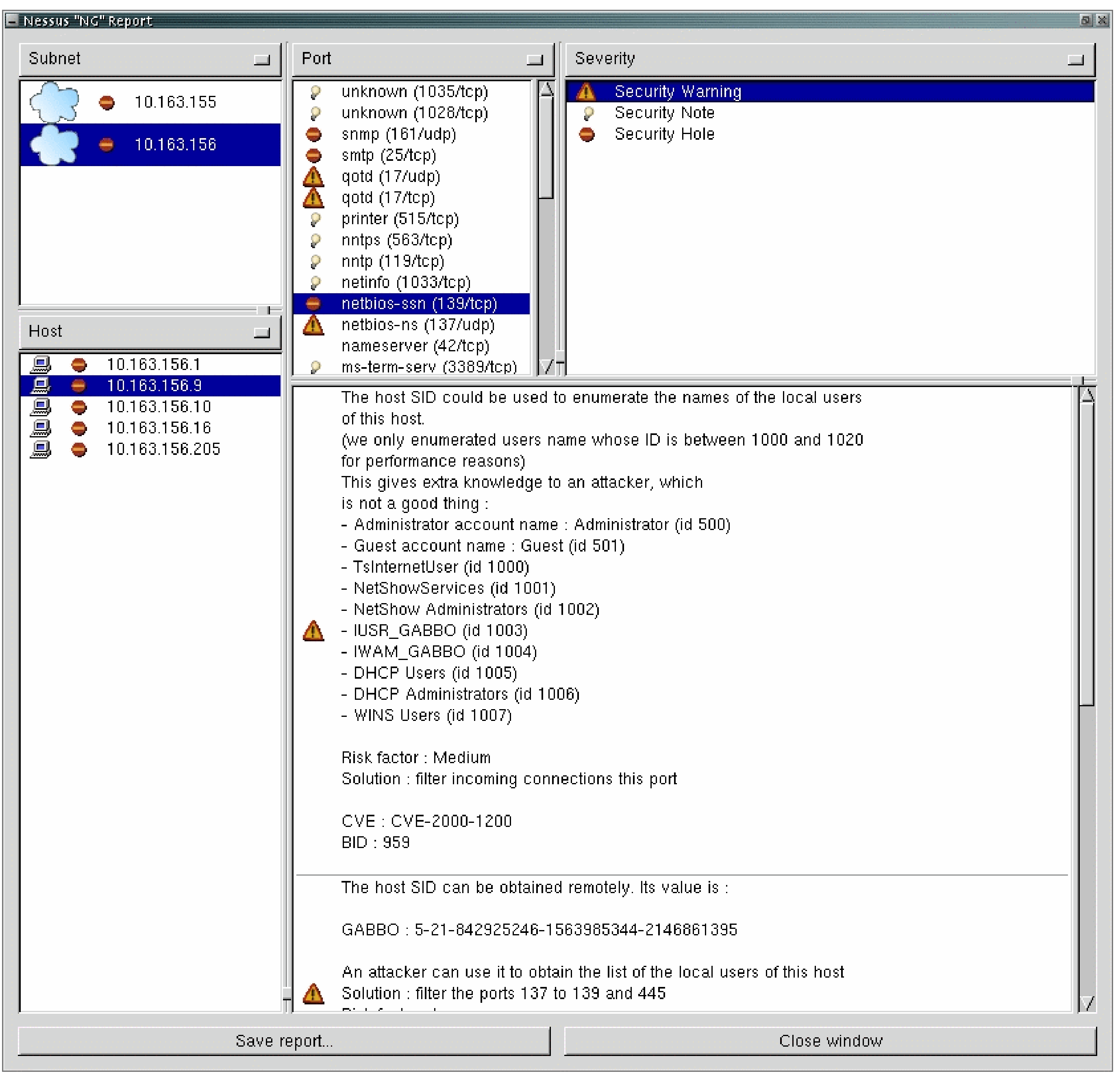
Nessus (4)

Scanning network from localhost

10.163.155.6	Attack :		
10.163.155.3	Portscan : Attack :		Stop
10.163.155.4	Portscan : Attack :		Stop
10.163.155.2	Portscan : Attack :		Stop
10.163.156.205	Portscan : Attack :		Stop
10.163.156.16	Portscan : Attack :		Stop
10.163.156.10	Portscan : Attack :		Stop
10.163.156.9	Portscan : Attack :		Stop
10.163.156.1	Portscan : Attack :		Stop

Stop the whole test

Nessus (5)



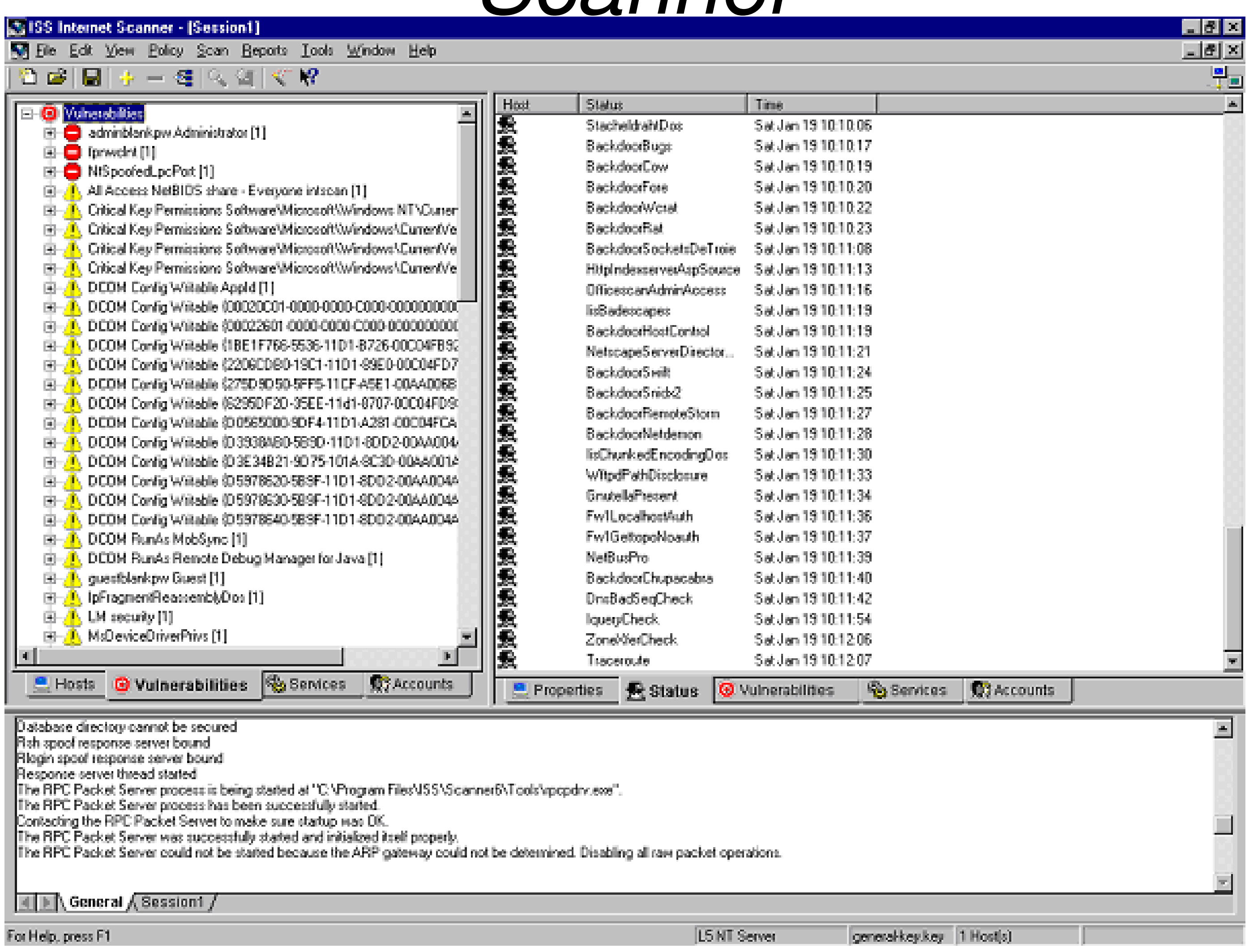
Nessus "NG" Report
Subnet
10.163.155
10.163.156
Host
10.163.156.1
10.163.156.9
10.163.156.10
10.163.156.16
10.163.156.205
Port
unknown (1035/tcp)
unknown (1028/tcp)
snmp (161/udp)
smtp (25/tcp)
qotd (17/udp)
qotd (17/tcp)
printer (515/tcp)
nntps (563/tcp)
nntp (119/tcp)
netinfo (1033/tcp)
netbios-ssn (139/tcp)
netbios-ns (137/udp)
nameserver (42/tcp)
ms-term-serv (3389/tcp)
Severity
Security Warning
Security Note
Security Hole
The host SID could be used to enumerate the names of the local users
of this host.
(we only enumerated users name whose ID is between 1000 and 1020
for performance reasons)
This gives extra knowledge to an attacker, which
is not a good thing :
- Administrator account name : Administrator (id 500)
- Guest account name : Guest (id 501)
- TsInternetUser (id 1000)
- NetShowServices (id 1001)
- NetShow Administrators (id 1002)
- IUSR_GABBO (id 1003)
- IWAM_GABBO (id 1004)
- DHCP Users (id 1005)
- DHCP Administrators (id 1006)
- WINS Users (id 1007)
Risk factor : Medium
Solution : filter incoming connections this port
CVE : CVE-2000-1200
BID : 959
The host SID can be obtained remotely. Its value is :
GABBO : 5-21-842925246-1563985344-2146861395
An attacker can use it to obtain the list of the local users of this host
Solution : filter the ports 137 to 139 and 445
Save report...
Close window

Nessus (6)

- Plusieurs formats de sortie
  - Interne (.NBE, .NSR)
  - HTML (2)
  - ASCII
  - LaTeX
- Consulter www.nessus.org (la page « Démonstration »)

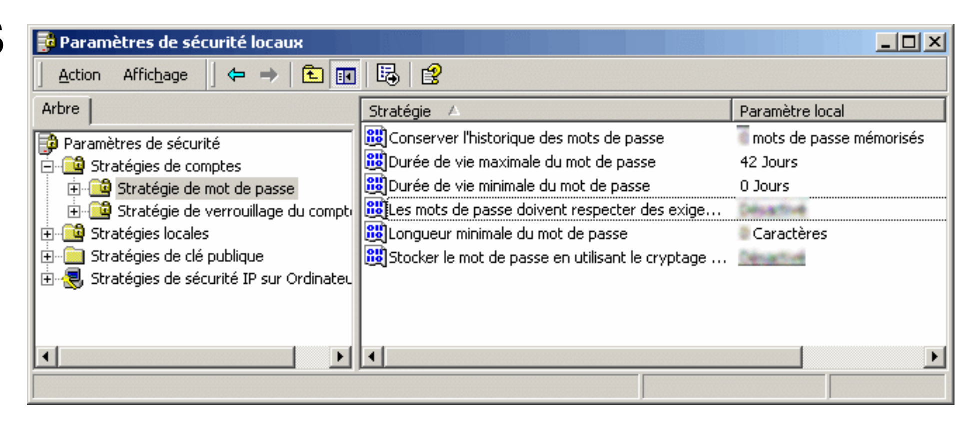
[Renaud Deraison *et al.*, 1998-2004]

ISS Internet/Wireless/System/Database Scanner



Mots de passe utilisés

- Étendre l'audit vers l'observation du niveau de vulnérabilité des mots de passe
- Attention à la protection des résultats
  - Il est probablement préférable de ne pas diffuser les résultats
- Associer ces résultats aux règles de gestion
  - Politique de préconisation
  - Sensibilisation
  - Règles automatiques



Plan (2/2)

- Protection utilisées dans la pratique
  - Protection réseau et *firewall*
  - Systèmes d'authentification
  - Chiffrement de flux et VPN
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
  - Détection d'intrusion
  - Audit, tests d'intrusion
  - **Administration, exploitation et suivi de la sécurité**
  - Observation et surveillance
- Protection des applications usuelles

Administration

- Configuration cohérente de nombreux éléments
- Correctifs (automatiques)
- Mise à jours (TFTP, etc.)
- Prise en main distante
  - SSH
  - VNC, Patrol, etc.
- Déport des traces (syslog)

Organisation (Fonctions)

- Administration système
  - Monde Unix
  - Monde Windows
- Administration BD
- Administrateurs applications
- Administration réseau
  - Commutation (LAN)
  - Routage (WAN)
- *Administration sécurité*
- Administration services d'infrastructure
  - DHCP, Active Directory
  - DNS
  - Sauvegardes
- Gestion des postes de travail
  - Configurations types, fabrication
  - Mise à disposition
  - Dépannage, incidents

Des éléments différents

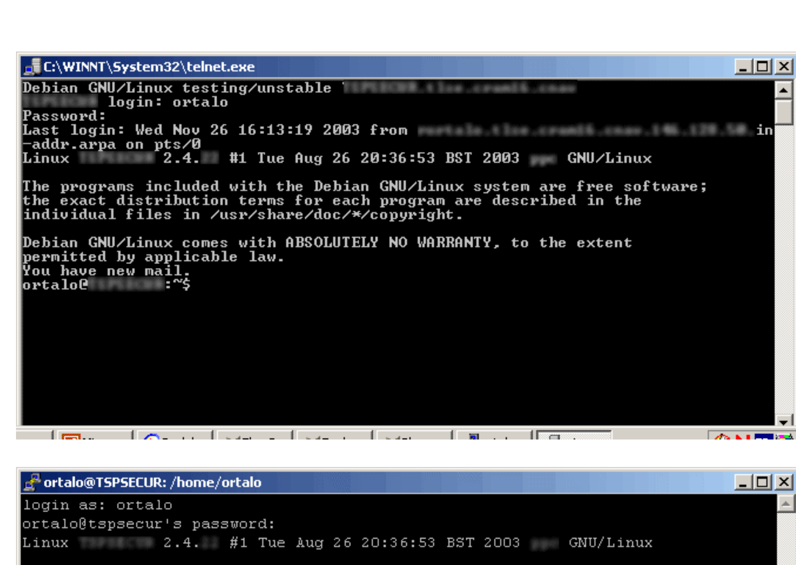
- Serveurs
  - UNIX
    - Solaris
    - Linux
      - RedHat
      - Suse
      - Debian
    - AIX
  - Windows
  - Novell
- Baies de disques
- Routeurs
- *Switches*
- PC Windows
- Macintosh
- Robots (sauvegardes)
- Imprimantes
- Boîtiers caches
- Boîtiers *firewall*
- Éléments logiciels
  - Antivirus
  - SGBD
  - …
- IDS

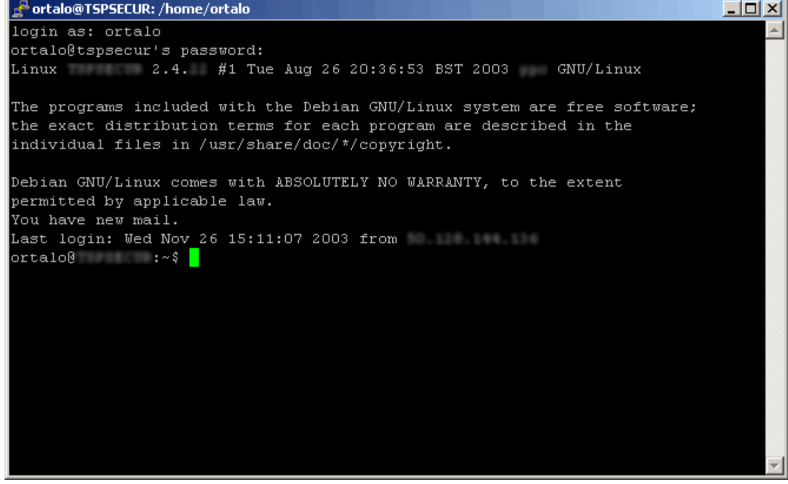
Correctifs et mises à jours

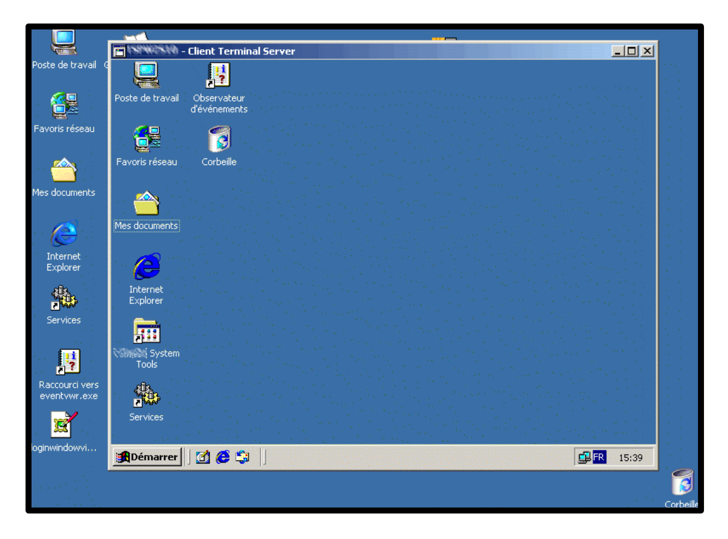
- Contraintes : ne pas perturber le fonctionnement normal
- Réagir (notamment à des alertes de sécurité)
- Faciliter les déploiements
  - *patches*
  - *Windows Update, SMS*
  - Lien avec les autres éléments du poste de travail ou des serveurs

Prise en main à distance

- Unix
  - Telnet, RSH *versus* SSH
- HTTP et HTTPS
- Windows
  - *Terminal Server*
  - VNC & co.







Systèmes embarqués

- Il s'agit souvent des équipements associés à *l'infrastructure réseau* (LAN)
- TFTP est largement répandu
  - Mise à jour des OS embarqués (*switch* Cisco, PIX)
  - Sauvegarde des configurations
- HTTP et HTTPS également (IHM)
- SNMP est supporté de manière hétérogène
- SSH apparaît sur les équipements réseau
- Équipements personnels ou PME, et ...

Plan (2/2)

- Protection utilisées dans la pratique
  - Protection réseau et *firewall*
  - Systèmes d'authentification
  - Chiffrement de flux et VPN
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
  - Détection d'intrusion
  - Audit, tests d'intrusion
  - Administration, exploitation et suivi de la sécurité
  - **Observation et surveillance**
- Protection des applications usuelles

Centralisation des traces

- Solutions propriétaires
- Syslog
- CNIL

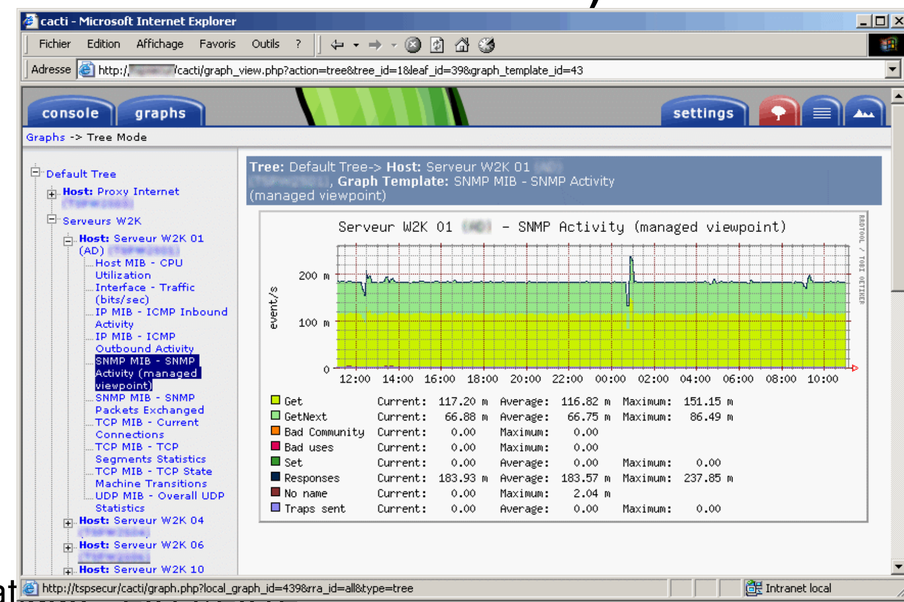
```
ortalo@[redacted]: /home/ortalo
Nov 27 10:02:02 [redacted] postgres[23600]: [1] LOG:  connection received: host=[local]
Nov 27 10:02:02 [redacted] postgres[23600]: [2] LOG:  connection authorized: user=postgres database=phpgroupware
Nov 27 10:02:08 [redacted] postgres[23608]: [1] LOG:  connection received: host=[local]
Nov 27 10:02:08 [redacted] postgres[23608]: [2] LOG:  connection authorized: user=postgres database=prelude
Nov 27 10:02:12 [redacted] postgres[23613]: [1] LOG:  connection received: host=[local]
Nov 27 10:02:12 [redacted] postgres[23613]: [2] LOG:  connection authorized: user=postgres database=template1
Nov 27 10:02:34 [redacted] nagios: SERVICE ALERT: [redacted];PING;OK;SOFT;3;PING OK - Packet loss = 0%, RTA = 117.51 ms
Nov 27 10:03:04 [redacted] nagios: SERVICE ALERT: [redacted];PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0%, RTA = 2
53.35 ms
Nov 27 10:04:04 [redacted] nagios: SERVICE ALERT: [redacted];PING;OK;SOFT;2;PING OK - Packet loss = 0%, RTA = 59.94 ms
Nov 27 10:05:01 [redacted] /USR/SBIN/CRON[24114]: (www-data) CMD (php4 /usr/share/cacti-0.8.3a/cmd.php > /dev/null 2>&
1)
Nov 27 10:05:23 [redacted] syslog-ng[198]: STATS: dropped 0
Nov 27 10:07:44 [redacted] nagios: HOST ALERT: [redacted];DOWN;SOFT;1;CRITICAL - Plugin timed out after 10 seconds
Nov 27 10:07:44 [redacted] nagios: HOST ALERT: [redacted];UP;SOFT;2;PING OK - Packet loss = 0%, RTA = 54.46 ms
Nov 27 10:07:44 [redacted] nagios: SERVICE ALERT: [redacted];PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0%, RTA =
 379.32 ms
Nov 27 10:08:01 [redacted] /USR/SBIN/CRON[24687]: (mail) CMD (  if [ -x /usr/lib/exim/exim3 -a -f /etc/exim/exim.conf
]; then /usr/lib/exim/exim3 -q ; fi)
Nov 27 10:08:35 [redacted] nagios: SERVICE ALERT: [redacted];PING;CRITICAL;SOFT;2;PING CRITICAL - Packet loss = 0%, RTA
 = 605.51 ms
Nov 27 10:08:54 [redacted] nagios: SERVICE ALERT: [redacted];PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0%, RTA = 2
06.12 ms
:
```

Observation et Surveillance

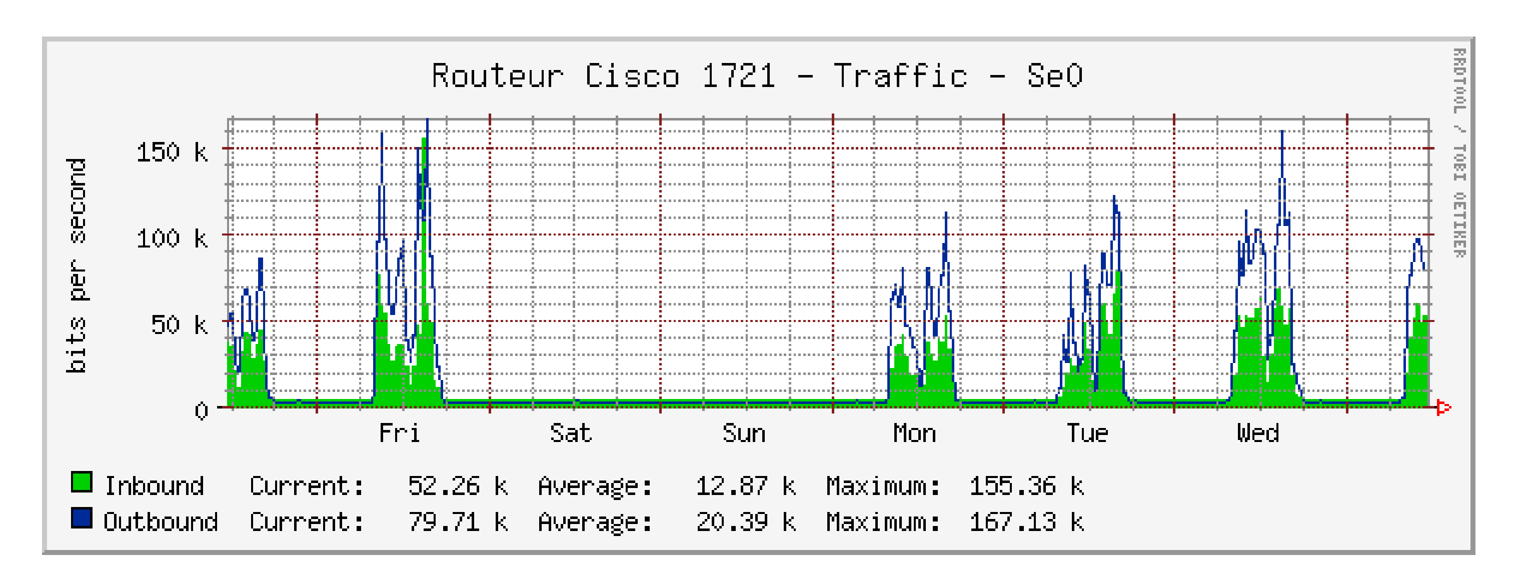
- *Monitoring* réseau
  - Équipements de sécurité
  - Autres équipements (réseaux et QoS par exemple)
- Surveillance système
- Évènements anormaux

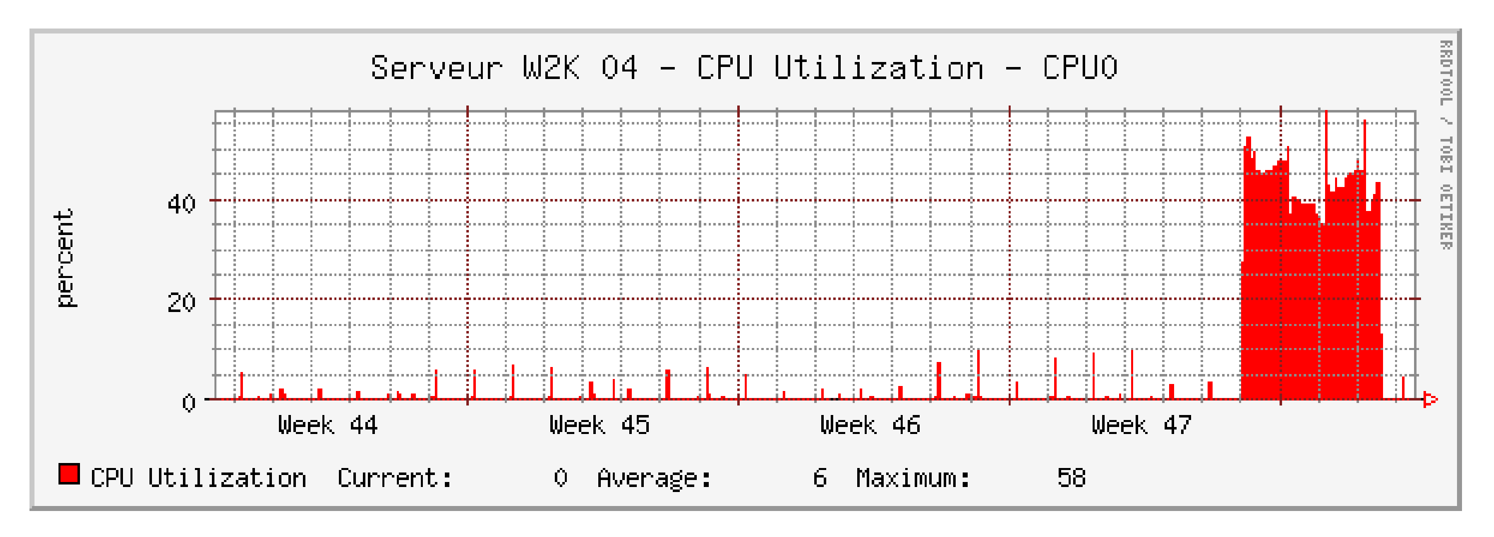
SNMP

- IF-MIB, HOST-MIB, etc. (www.mibdepot.com)
- NET-SNMP, UCD-SNMP, IETF Cisco, 3Com, Nortell, IBM, etc.
- RRDTool, MRTG, Cacti, HPoV, Tivoli, etc.
- Requêtes (sur UDP/161 et UDP/162):
  - Get
  - GetNext
  - Set
  - Response
  - Trap

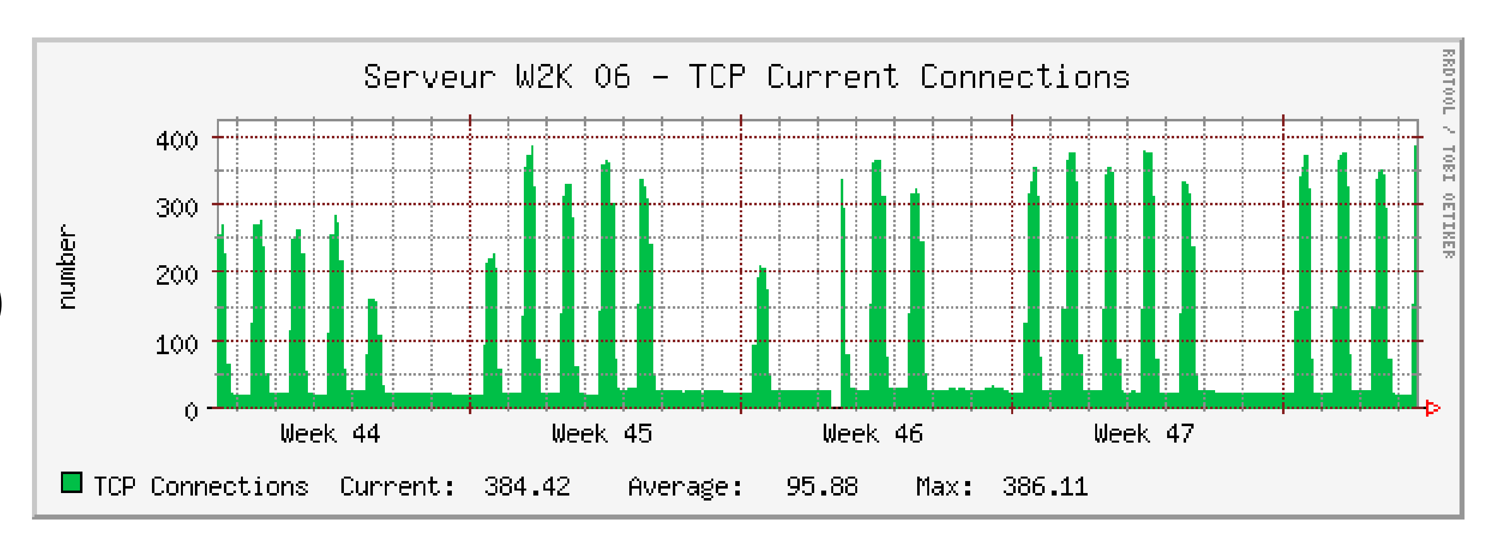


SNMP (Exemples)





SNMP
(Exemples)



Serveur W2K 01 (AD) - ICMP Inbound Activity

message/s

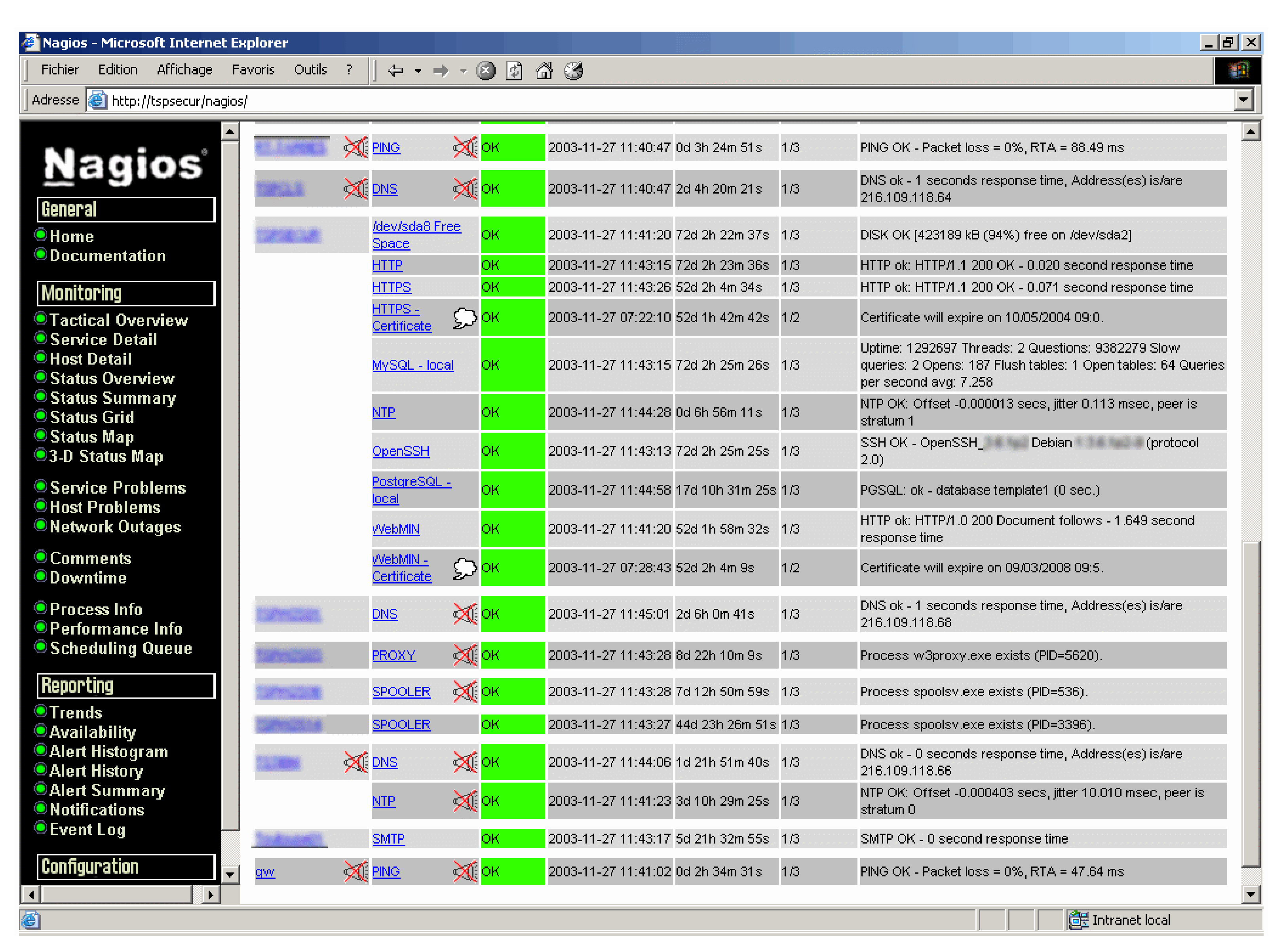
1.5
1.0
0.5
0.0

12:00 14:00 16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00

RRDTOOL / TOBI OETIKER

Errors	Current:	0.00	Average:	0.00	Maximum:	0.00
Dest. Unreach.	Current:	10.24 m	Average:	14.68 m	Maximum:	1.12
Echo Request	Current:	207.16 m	Average:	121.04 m	Maximum:	277.37 m
Echo Reply	Current:	39.57 m	Average:	44.17 m	Maximum:	64.87 m
Shown - Total	Current:	4.56 m	Average:	1.88 m	Maximum:	13.04 m
Total In	Current:	261.53 m	Average:	181.76 m	Maximum:	1.36

Surveillance système (exemple)



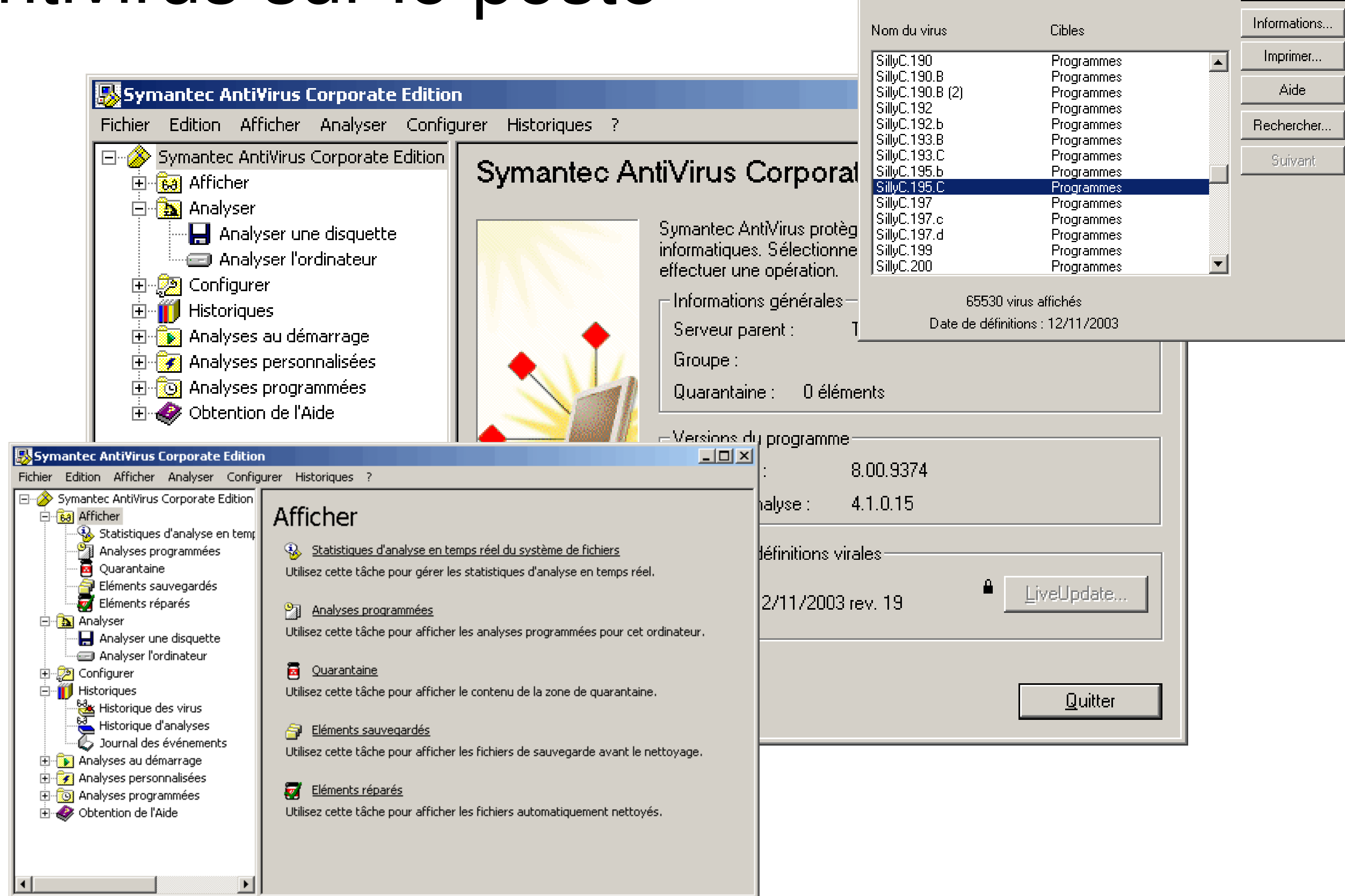
Plan (2/2)

- Protection utilisées dans la pratique
  - Protection réseau et *firewall*
  - Systèmes d'authentification
  - Chiffrement de flux et VPN
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
  - Détection d'intrusion
  - Audit, tests d'intrusion
  - Administration, exploitation et suivi de la sécurité
  - Observation et surveillance
- **Protection des applications usuelles**

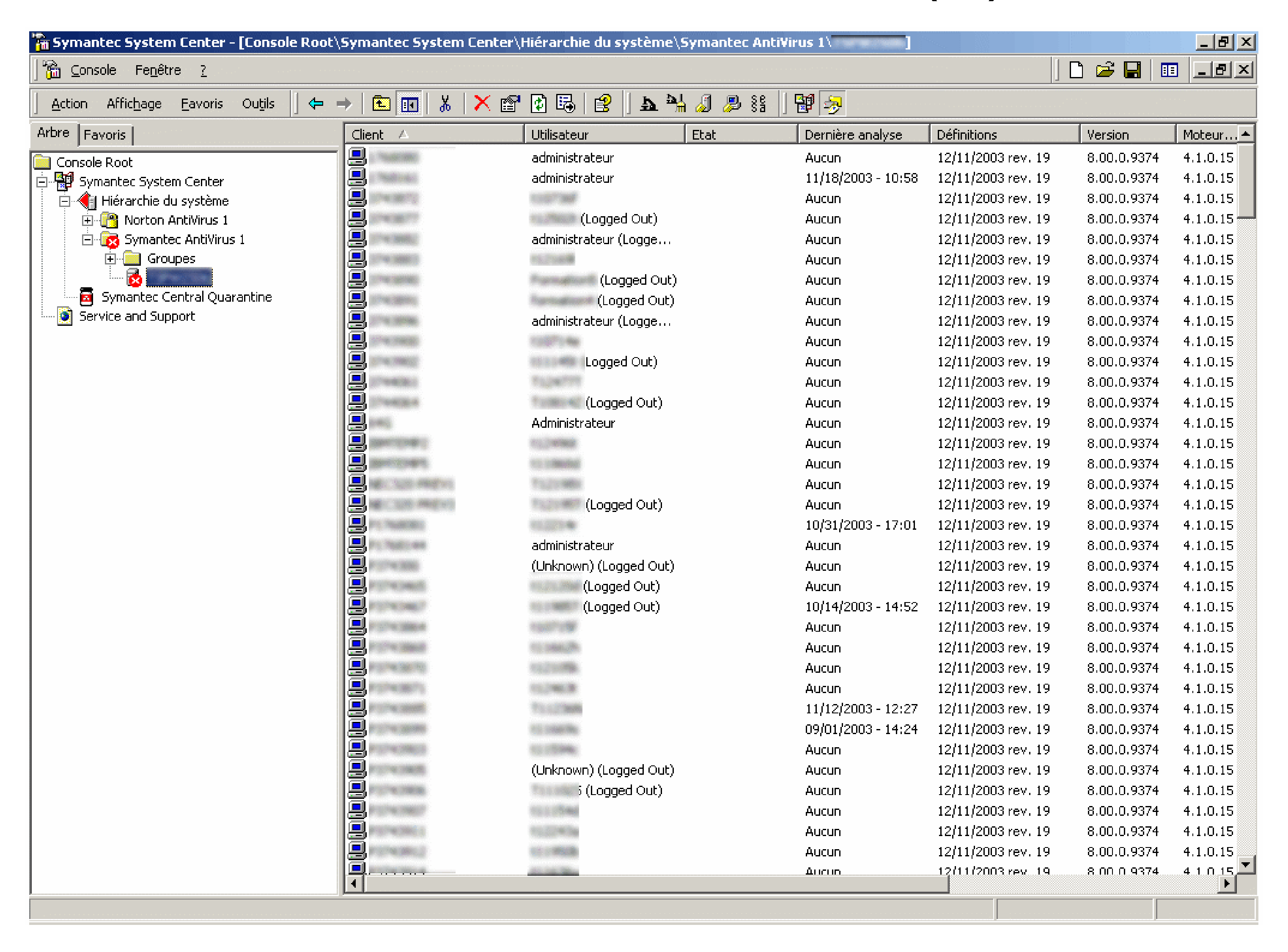
Plan (détaillé)

- **Protection des applications (usuelles)**
  - Poste de travail : antivirus
  - *Messagerie, Flux HTTP (entrant) : antivirus*
  - Serveur HTTP
  - Flux HTTP (sortant) : filtrage d'URL
  - *Services Internet : e-* et HTTPS*
  - *Services Internet : e-* Pro (Portal, WebSphere, SOAP & co.)*
  - Signature et messagerie (S/MIME, OpenPGP)
  - DNS (et DNSSEC)
  - *Routage IP (OSPF, RIP, BGP)*
  - Infrastructure SSI : PKI, X.509, LDAP, etc.

Antivirus sur le poste

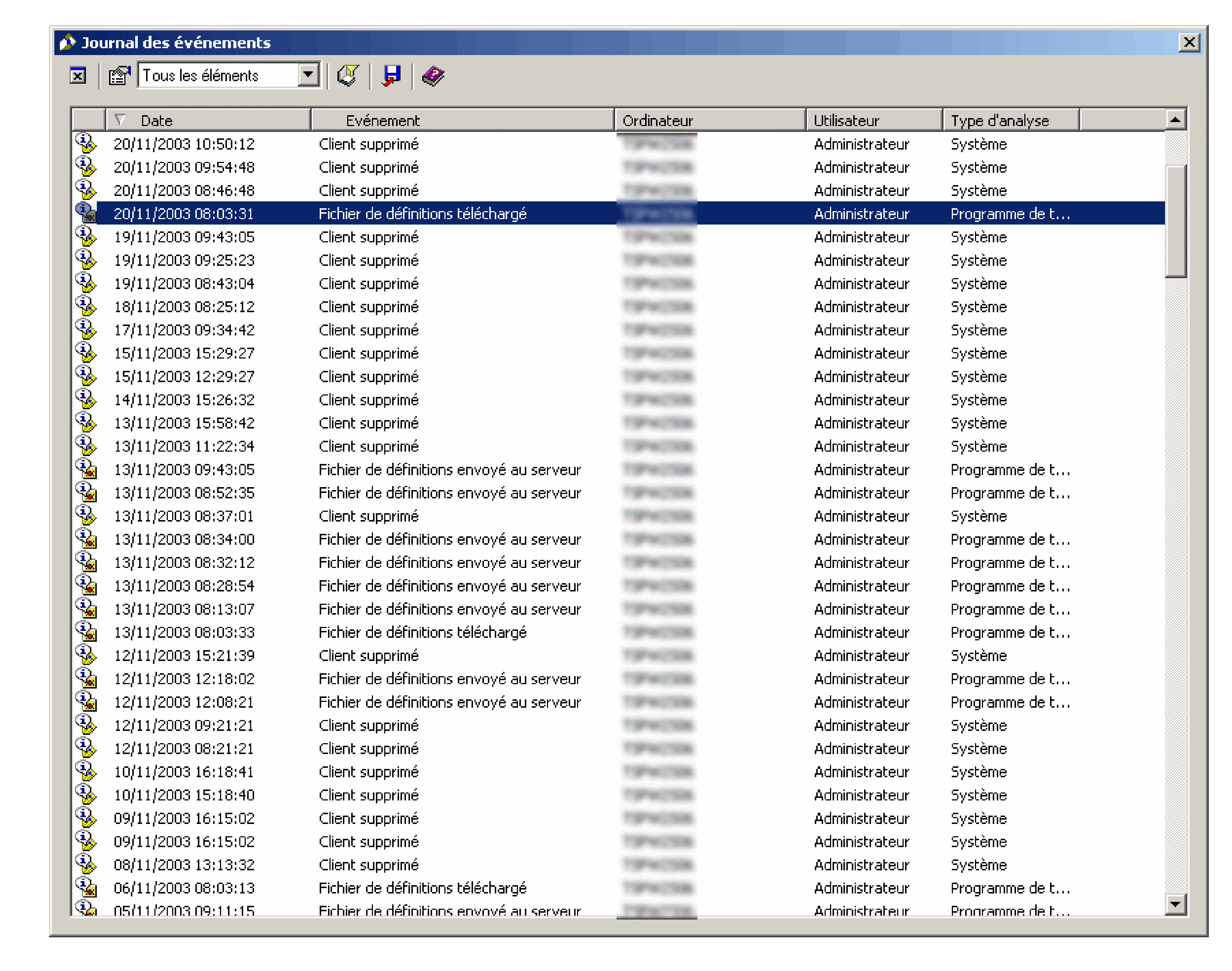


Console Antivirus (1)



Client	Utilisateur	Etat	Dernière analyse	Définitions	Version	Moteur…
	administrateur		Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
	administrateur		11/18/2003 - 10:58	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
	(Logged Out)		Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
	administrateur (Logge…		Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
	(Logged Out)		Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
	(Logged Out)		Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
	administrateur (Logge…		Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
	Logged Out)		Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
	(Logged Out)		Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
	Administrateur		Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
	(Logged Out)		Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			10/31/2003 - 17:01	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
	administrateur		Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
	(Unknown) (Logged Out)		Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
	(Logged Out)		Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
	(Logged Out)		10/14/2003 - 14:52	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			11/12/2003 - 12:27	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			09/01/2003 - 14:24	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
	(Unknown) (Logged Out)		Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
	(Logged Out)		Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15
			Aucun	12/11/2003 rev. 19	8.00.0.9374	4.1.0.15

Console Antivirus (2)



Date	Evénement	Ordinateur	Utilisateur	Type d'analyse
20/11/2003 10:50:12	Client supprimé	[illegible]	Administrateur	Système
20/11/2003 09:54:48	Client supprimé	[illegible]	Administrateur	Système
20/11/2003 08:46:48	Client supprimé	[illegible]	Administrateur	Système
20/11/2003 08:03:31	Fichier de définitions téléchargé	[illegible]	Administrateur	Programme de t...
19/11/2003 09:43:05	Client supprimé	[illegible]	Administrateur	Système
19/11/2003 09:25:23	Client supprimé	[illegible]	Administrateur	Système
19/11/2003 08:43:04	Client supprimé	[illegible]	Administrateur	Système
18/11/2003 08:25:12	Client supprimé	[illegible]	Administrateur	Système
17/11/2003 09:34:42	Client supprimé	[illegible]	Administrateur	Système
15/11/2003 15:29:27	Client supprimé	[illegible]	Administrateur	Système
15/11/2003 12:29:27	Client supprimé	[illegible]	Administrateur	Système
14/11/2003 15:26:32	Client supprimé	[illegible]	Administrateur	Système
13/11/2003 15:58:42	Client supprimé	[illegible]	Administrateur	Système
13/11/2003 11:22:34	Client supprimé	[illegible]	Administrateur	Système
13/11/2003 09:43:05	Fichier de définitions envoyé au serveur	[illegible]	Administrateur	Programme de t...
13/11/2003 08:52:35	Fichier de définitions envoyé au serveur	[illegible]	Administrateur	Programme de t...
13/11/2003 08:37:01	Client supprimé	[illegible]	Administrateur	Système
13/11/2003 08:34:00	Fichier de définitions envoyé au serveur	[illegible]	Administrateur	Programme de t...
13/11/2003 08:32:12	Fichier de définitions envoyé au serveur	[illegible]	Administrateur	Programme de t...
13/11/2003 08:28:54	Fichier de définitions envoyé au serveur	[illegible]	Administrateur	Programme de t...
13/11/2003 08:13:07	Fichier de définitions envoyé au serveur	[illegible]	Administrateur	Programme de t...
13/11/2003 08:03:33	Fichier de définitions téléchargé	[illegible]	Administrateur	Programme de t...
12/11/2003 15:21:39	Client supprimé	[illegible]	Administrateur	Système
12/11/2003 12:18:02	Fichier de définitions envoyé au serveur	[illegible]	Administrateur	Programme de t...
12/11/2003 12:08:21	Fichier de définitions envoyé au serveur	[illegible]	Administrateur	Programme de t...
12/11/2003 09:21:21	Client supprimé	[illegible]	Administrateur	Système
12/11/2003 08:21:21	Client supprimé	[illegible]	Administrateur	Système
10/11/2003 16:18:41	Client supprimé	[illegible]	Administrateur	Système
10/11/2003 15:18:40	Client supprimé	[illegible]	Administrateur	Système
09/11/2003 16:15:02	Client supprimé	[illegible]	Administrateur	Système
09/11/2003 16:15:02	Client supprimé	[illegible]	Administrateur	Système
08/11/2003 13:13:32	Client supprimé	[illegible]	Administrateur	Système
06/11/2003 08:03:13	Fichier de définitions téléchargé	[illegible]	Administrateur	Programme de t...
05/11/2003 09:11:15	Fichier de définitions envoyé au serveur	[illegible]	Administrateur	Programme de t...

Console Antivirus (3)

Historique des virus

Tous les éléments

	Date	Nom du fichier	Nom du virus	Type de virus	Opération effect...
	20/11/2003 23:32:25	EuroConverter.ZIP		Fichier compressé	Déplacé
	20/11/2003 23:32:25	EuroConverter/Setup.exe	W95.Hybris.worm	Fichier; Fichier ...	Déplacé
	20/11/2003 23:32:13	add on euro acces.zip		Fichier compressé	Déplacé
	20/11/2003 23:32:13	Setup.exe	W95.Hybris.worm	Fichier; Fichier ...	Déplacé
	15/10/2003 09:06:47	RECUP2.DOC	Macro Component	Fichier; Macro	Nettoyé
	15/10/2003 08:55:33	RECUP2.DOC	Macro Component	Fichier; Macro	Nettoyé
	25/09/2003 09:00:03	TFTP1244	W32.Blaster.Worm	Fichier	Supprimé
	25/09/2003 08:59:23	TFTP1192	W32.Blaster.Worm	Fichier	Supprimé
	25/09/2003 08:58:36	TFTP784	W32.Blaster.Worm	Fichier	Supprimé
	25/09/2003 08:58:30	TFTP384	W32.Blaster.Worm	Fichier	Supprimé
	25/09/2003 08:57:45	TFTP828	W32.Blaster.Worm	Fichier	Supprimé
	25/09/2003 08:57:18	TFTP988	W32.Blaster.Worm	Fichier	Supprimé
	25/09/2003 08:56:33	TFTP1128	W32.Blaster.Worm	Fichier	Supprimé
	25/09/2003 08:56:02	TFTP1252	W32.Blaster.Worm	Fichier	Supprimé
	25/09/2003 08:55:52	TFTP452	W32.Blaster.Worm	Fichier	Supprimé
	25/09/2003 08:55:43	TFTP400	W32.Blaster.Worm	Fichier	Supprimé
	25/09/2003 08:55:27	TFTP692	W32.Blaster.Worm	Fichier	Supprimé
	25/09/2003 08:54:37	TFTP628	W32.Blaster.Worm	Fichier	Supprimé
	25/09/2003 08:53:53	TFTP732	W32.Blaster.Worm	Fichier	Supprimé
	25/09/2003 08:52:55	TFTP1380	W32.Blaster.Worm	Fichier	Supprimé
	25/09/2003 08:52:44	TFTP396	W32.Blaster.Worm	Fichier	Supprimé
	25/09/2003 08:52:42	TFTP1272	W32.Blaster.Worm	Fichier	Supprimé

Serveur Web

- Serveur HTTP et serveur HTTPS
- Sélection des utilisateurs
  - Plages d'adresses
  - Certificats
- Sélection des destinations
  - Chemin d'accès
  - Type d'extension
- Maîtrise des extensions dynamiques
- Contrôle du processus serveur
  - Confinement
  - Lien avec le système de fichiers

Apache 1.3 (1)

- Configuration réseau fondamentale

  [Debian 3.1]

  #**Listen** 3000

  #**Listen** 12.34.56.78:80

  #BindAddress *

  Port 80 (?)
- Extensions (modules)

  LoadModule cgi_module /usr/lib/apache/1.3/mod_cgi.so

  # LoadModule asis_module /usr/lib/apache/1.3/mod_asis.so

  LoadModule alias_module /usr/lib/apache/1.3/**mod_alias**.so

  LoadModule access_module
  /usr/lib/apache/1.3/**mod_access**.so

  LoadModule php4_module /usr/lib/apache/1.3/libphp4.so
- Processus

  User www-data

  Group www-data

Apache 1.3 (2)

- Configuration conditionnelle
  <IfModule mod_status.c>
    ExtendedStatus On
  </IfModule>
- Configuration modulaire
  Include /etc/phpmyadmin/apache.conf
  Include /etc/phpgroupware/apache.conf
- Directives de contexte
  <Directory> et <DirectoryMatch>
  <Files> et <FilesMatch>
  <Location> et <LocationMatch>
  <VirtualHost>

Apache 1.3 (3)

- Contrôle des chemins d'accès (fichiers)

  <**Directory** />
  Options SymLinksIfOwnerMatch
  AllowOverride None
  </Directory>
  …
  <**Directory** /var/www/>
  Options Indexes Includes FollowSymLinks MultiViews
  AllowOverride None
  Order allow,deny
  Allow from all
  </Directory>
  …

<**Directory** /home/*/public_html>
AllowOverride FileInfo AuthConfig Limit
Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
<**Limit** GET POST OPTIONS PROPFIND>
Order allow,deny
Allow from all
</Limit>
<**Limit** PUT DELETE PATCH PROPPATCH MKCOL COPY MOVE LOCK UNLOCK>
Order deny,allow
Deny from all
</Limit>
</Directory>

Apache 1.3 (4)

- Contrôle des noms de fichiers

```
<Files ~ "^\.ht">
    Order allow,deny
    Deny from all
</Files>
```

- A vérifier

```
# If the perl module is installed,
  this will be enabled.
<IfModule mod_perl.c>
 Alias /perl/ /var/www/perl/
 <Location /perl>
  SetHandler perl-script
  PerlHandler
  Apache::Registry
  Options +ExecCGI
 </Location>
</IfModule>
```

Apache 1.3 (5)

- Contrôle des chemins d'accès (URL)

  Alias /doc/ /usr/share/doc/

  <**Location** /doc>

  order deny,allow

  deny from all

  allow from 127.0.0.0/255.0.0.0

  allow from AA.BB.CC.0/255.255.XX.0

  Options Indexes FollowSymLinks MultiViews

  </Location>

  …

For Prelude PIWI

Alias /piwi /home/*xxxx*/prelude/piwi

ScriptAlias /piwi /home/*xxxx*/prelude/piwi

<DirectoryMatch /home/*xxxx*/prelude/piwi/>

order allow,deny

allow from all

Options +ExecCGI

AddHandler cgi-script .pl

DirectoryIndex **index.pl**

</DirectoryMatch>

Apache 1.3 (6)

- /etc/phpgroupware/apache.conf

```
Alias /phpgroupware /usr/share/phpgroupware
<Directory /usr/share/phpgroupware/>
        Options +FollowSymLinks
        AllowOverride None
        order allow,deny
        allow from all
        DirectoryIndex index.html index.php
        <IfModule mod_php3.c>
                php3_magic_quotes_gpc On
                php3_track_vars On
                php3_include_path .:/etc/phpgroupware
        </IfModule>
        <IfModule mod_php4.c>
                php_flag magic_quotes_gpc On
                php_flag track_vars On
                php_flag session.save_path /var/tmp/phpgroupware
                php_value include_path .:/etc/phpgroupware
        </IfModule>
</Directory>
```

Exemple de fichier de configuration secondaire

Apache 1.3 (7)

- *Virtual hosts*
  - # VirtualHost example:
  - # *Almost* any Apache directive may go into a VirtualHost container.
  - #
  - #<**VirtualHost** ip.address.of.host.some_domain.com>
  - #   ServerAdmin webmaster@host.some_domain.com
  - #   **DocumentRoot** /www/docs/host.some_domain.com
  - #   **ServerName** host.some_domain.com
  - #   ErrorLog logs/host.some_domain.com-error.log
  - #   CustomLog logs/host.some_domain.com-access.log common
  - #</VirtualHost>
- Consulter la documentation
- N’oubliez pas Apache-SSL

Le *proxy* Web

- Le relais le plus utilisé dans un système d'information
- Couplé à du filtrage d'URL (nécessairement)
- Liaison souhaitable avec l'authentification du poste de travail
- Fonction de cache

Squid – Règles de contrôle d’accès

www.squid-cache.org

- Deux composants
  - Éléments (*ACL elements*)
  - Règles (*access lists rules*)
- Combinaison

  acl_type {**allow**|**deny**} *acl* AND *acl* AND ...

  OR *acl_type* {**allow**|**deny**} *acl* AND *acl* AND ...

  OR ...
- Exemples (utiles)
  - ```
    acl all src 0/0
    http_access deny all
    ```
  - ```
    acl myclients src 1.2.3.0/24
    http_access allow myclients
    ```

Squid – ACL *elements*

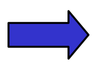
Squid knows about the following types of ACL elements :

- **src**: source (client) IP addresses
- **dst**: destination (server) IP addresses
- **myip**: the local IP address of a client's connection
- **srcdomain**: source (client) domain name
- **dstdomain**: destination (server) domain name
- **srcdom_regex**: source (client) regular expression pattern matching
- **dstdom_regex**: destination (server) regular expression pattern matching
- **time**: time of day, and day of week
- **url_regex**: URL regular expression pattern matching
- **urlpath_regex**: URL-path regular expression pattern matching, leaves out the protocol and hostname
- **port**: destination (server) port number
- **myport**: local port number that client connected to
- **proto**: transfer protocol (http, ftp, etc)
- **method**: HTTP request method (get, post, etc)
- **browser**: regular expression pattern matching on the request's user-agent header
- **ident**: string matching on the user's name
- **ident_regex**: regular expression pattern matching on the user's name
- **src_as**: source (client) Autonomous System number
- **dst_as**: destination (server) Autonomous System number
- **proxy_auth**: user authentication via external processes
- **proxy_auth_regex**: user authentication via external processes
- **snmp_community**: SNMP community string matching
- **maxconn**: a limit on the maximum number of connections from a single client IP address
- **req_mime_type**: regular expression pattern matching on the request content-type header
- **arp**: Ethernet (MAC) address matching
- **rep_mime_type**: regular expression pattern matching on the reply (downloaded content) content-type header. This is only usable in the *http_reply_access* directive, not *http_access*.
- **external**/: lookup via external acl helper defined by external_acl_type

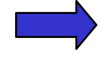
Note: The information here is current for version 2.5

Squid – *Access lists types*

There are a number of different access lists:



- **http_access**: Allows HTTP clients (browsers) to access the HTTP port. This is the primary access control list.
- **http_reply_access**: Allows HTTP clients (browsers) to receive the reply to their request. This further restricts permissions given by http_access, and is primarily intended to be used together with the rep_mime_type acl type for blocking different content types.
- **icp_access**: Allows neighbor caches to query your cache with ICP.
- **miss_access**: Allows certain clients to forward cache misses through your cache. This further restricts permissions given by http_access, and is primarily intended to be used for enforcing sibling relations by denying siblings from forwarding cache misses through your cache.
- **no_cache**: Defines responses that should not be cached.
- **redirector_access**: Controls which requests are sent through the redirector pool.
- **ident_lookup_access**: Controls which requests need an Ident lookup.



- **always_direct**: Controls which requests should always be forwarded directly to origin servers.
- **never_direct**: Controls which requests should never be forwarded directly to origin servers.
- **snmp_access**: Controls SNMP client access to the cache.
- **broken_posts**: Defines requests for which squid appends an extra CRLF after POST message bodies as required by some broken origin servers.
- **cache_peer_access**: Controls which requests can be forwarded to a given neighbor (peer).

SquidGuard (1)

www.squidguard.org

- Un redirecteur pour Squid
- Recherche efficace pour des listes de grandes tailles (>100 000 entrées)
- Définition de listes de contrôle d’accès
- Prise en compte des plages horaires
- Propose des listes noires d’URL et de sites (et un robot)

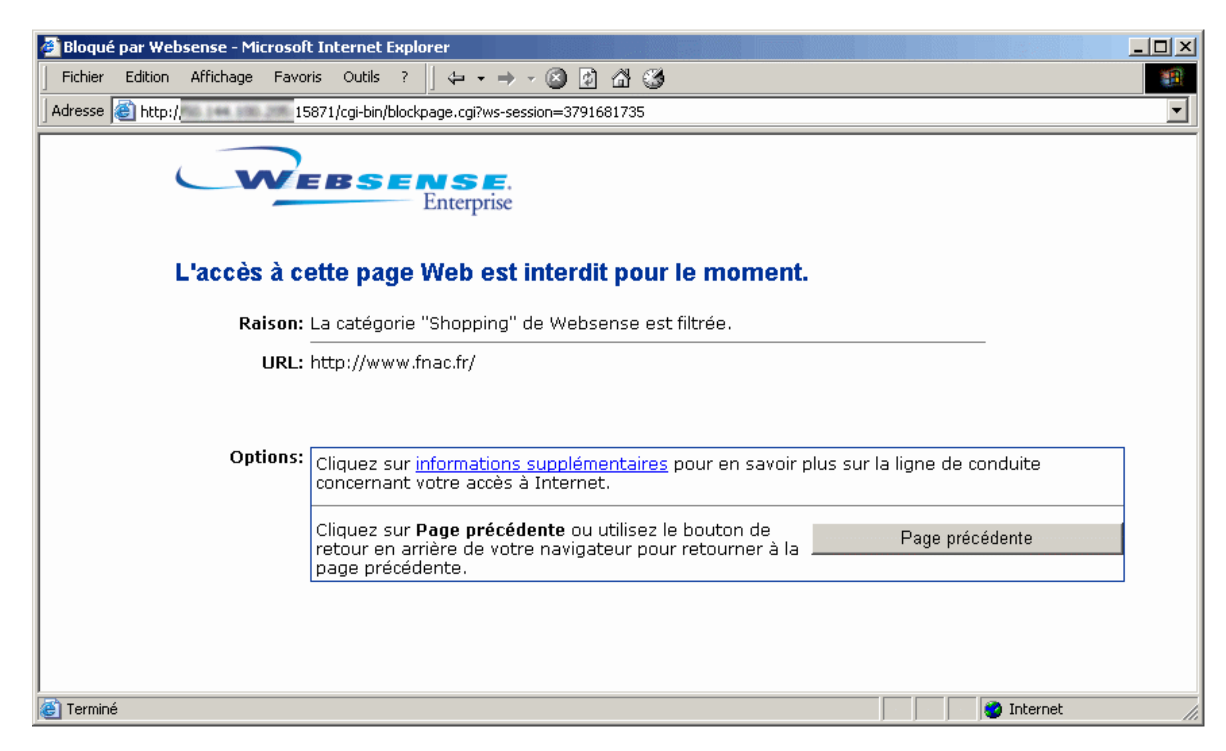
SquidGuard (2)

- Exemple:

```
logdir /usr/local/squidGuard/log
dbhome /usr/local/squidGuard/db
src grownups { ip 10.0.0.0/24 user foo bar }
src kids { ip 10.0.1.0/24 }
dest porn { domainlist porn/domains urllist porn/urls }
acl {
    grownups { pass all }
    kids { pass !porn all }
    default {
       pass none
       redirect http://info.foo.bar/cgi/blocked?clientaddr=
    %a&clientname=%n&
           clientuser=%i&clientgroup=%s&targetgroup=%t&url=%u
    }
}
```

Filtrage d'URL

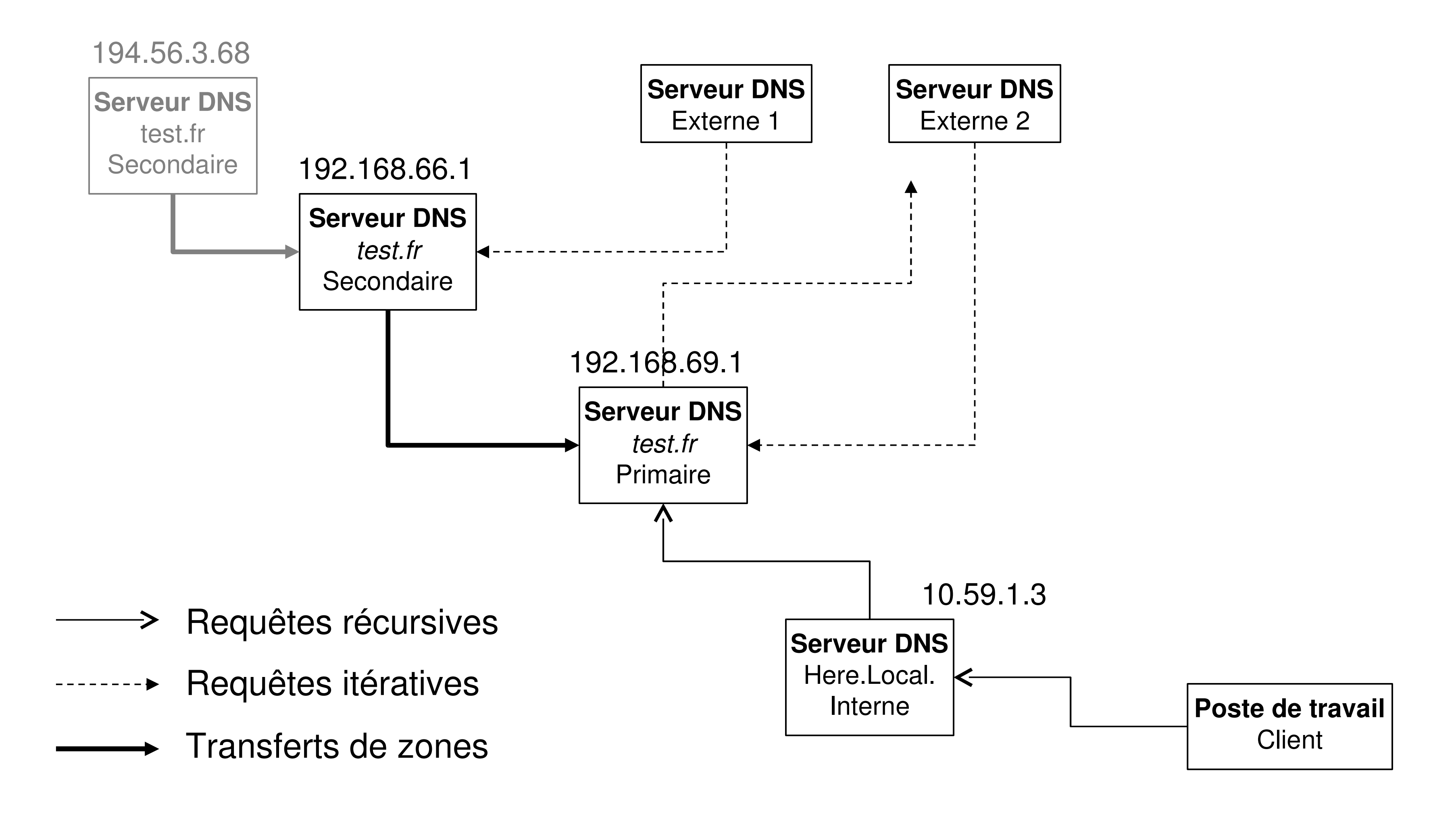
- Les offres commerciales incluent la classification des sites
- Exemple : WebSense



DNS

- Sécuriser les échanges entre les serveurs eux-mêmes
- Contrôler correctement les clients
- Émettre efficacement les requêtes
- Organiser précisément la diffusion de l'information gérée (notamment en présence de translation d'adresses)

DNS : test.fr.


194.56.3.68
Serveur DNS
test.fr
Secondaire
192.168.66.1
Serveur DNS
test.fr
Secondaire
Serveur DNS
Externe 1
Serveur DNS
Externe 2
192.168.69.1
Serveur DNS
test.fr
Primaire
10.59.1.3
Serveur DNS
Here.Local.
Interne
Poste de travail
Client
Requêtes récursives
Requêtes itératives
Transferts de zones

DNS et BIND

- BIND 8
- BIND 9
  - Possibilités d’authentification forte
    - Échanges entre serveurs
    - Administration
  - Transferts de zone incrémentaux
  - DNSSEC

BIND 9 (1)

- Limiter les transferts de zones

```
zone "test.fr" {
    type master;
    file "/etc/bind/db.test.fr";
    allow-transfer {
      192.168.66.1;
    };
};
```

- Même sur un secondaire

```
zone "test.fr" {
    type slave;
    masters { 192.168.69.1; };
    file "/etc/bind/bak.db.test.fr";
    allow-transfer {
      194.56.3.68; // or "none"
    };
};
```

BIND 9 (2)

- Contrôler les accès aux zones gérées
  - requêtes directes : autres serveurs
  - requêtes itératives : pour les clients finaux

```
// We allow only recursive queries from the internal
   nameserver and self
acl "ns_rzo" { 192.168.66.1; 10.59.1.3; 127.0.0.1; };
// We also allow the admin. station to do queries here directly
acl "admin" { 192.168.65.1; };
…
   allow-query { any; }; // or "slaves_ns"
   allow-recursion { "ns_rzo"; "admin"; };
```

BIND 9 (2)

- Fonctionner en mode relais pur

```
options {
…
    // Allowed forwarders (only the DMZ nameservers)
    forwarders {
      192.168.69.1; 192.168.66.1;
     };

    // We *always* forward
    forward only;
…
};
```

PGP et la confiance

- Un protocole : OpenPGP (RFC 2440)
- Deux principales implémentations : PGP et GnuPG
- Le conteneur contient : un bi-clef, un ensemble de signatures et des informations « administratives »
- Signer une clef
  - Cela signifie que vous avez pu vérifier *directement* l'identité du détenteur de la clef publique (par exemple à l'aide d'une empreinte de cette clef communiquée en personne et d'une carte d'identité)
  - Cela ne signifie rien d'autre
- Pour signer ou chiffrer des fichiers et des messages
- *Trust* : permet de limiter la transitivité (et indiquer ceux qui ne définissent pas « signer une clef » comme vous)

PKI – Autorités de certification

